DETERMINISTIC AND EFFICIENT THREE-PARTY QUANTUM KEY DISTRIBUTION

Muneer Alshowkan

Under the Supervision of Dr. Khaled Elleithy

DISSERTATION

SUBMITTED IN PARTIAL FULFILMENT OF THE REQUIREMENTS

FOR THE DEGREE OF DOCTOR OF PHILOSOPHY IN COMPUTER SCIENCE

AND ENGINEERING

THE SCHOOL OF ENGINEERING

UNIVERSITY OF BRIDGEPORT

CONNECTICUT

December, 2017

DETERMINISTIC AND EFFICIENT THREE-PARTY QUANTUM KEY DISTRIBUTION

Muneer Alshowkan

Under the Supervision of Dr. Khaled Elleithy

Approvals

Committee Members

Name	Signature	Date
Dr. Khaled Elleithy		12/18/17
Dr. Miad Faezipour		12,18,2017
Dr. Xingguo Xiong		01/12/2018
Dr. Junling Hu		12/18/17
Dr. Saeid Moslehpour		12,12,17

Ph.D. Program Coordinator

Dr. Khaled M. Elleithy		12/18/17

Chairman, Computer Science and Engineering Department

Dr. Ausif Mahmood		12/18/2017

Dean, School of Engineering

Dr. Tarek M. Sobh		11/8/2018

DETERMINISTIC AND EFFICIENT THREE-PARTY QUANTUM KEY DISTRIBUTION

DETERMINISTIC AND EFFICIENT THREE-PARTY QUANTUM KEY DISTRIBUTION

ABSTRACT

Quantum information processing is based on the laws of quantum physics and guarantees the unconditional security. In this thesis we propose an efficient and deterministic three-party quantum key distribution algorithm to establish a secret key between two users. Using the formal methodological approach, we study and model a quantum algorithm to distribute a secret key to a sender and a receiver when they only share entanglement with a trusted party but not with each other. It distributes a secret key by special pure quantum states using the remote state preparation and controlled gates. In addition, we employ the parity bit of the entangled pairs and ancillary states to help in preparing and measuring the secret states. Distributing a state to two users requires two maximally entangled pairs as the quantum channel and a two-particle von Neumann projective measurement. This protocol is exact and deterministic. It distributes a secret key of d qubits by $2d$ entangled pairs and on average d bits of classical communication. We show the security of this protocol against the entanglement attack and offer a method for privacy amplification.

Moreover, we also study the problem of distributing Einstein-Podolsky-Rosen (EPR) in a metropolitan network. The EPR is the building block of entanglement-based and entanglement-assisted quantum communication protocols. Therefore, prior shared EPR pair and an authenticated classical channel allow two distant users to share a secret key. To build a network architecture where a centralized EPR source creates entangled states by the process of spontaneous parametric down-conversion (SPDC) then routes the states to users in different access networks. We propose and simulate a metropolitan optical network (MON) architecture for entanglement distribution in a typical telecommunication infrastructure. The architecture allows simultaneous transmission of classical and quantum signals in the network and offers a dynamic routing mechanism to serve the entire metropolitan optical network.

ACKNOWLEDGEMENTS

First of all, I would like to thank my parents, brothers and sisters. They provide me with their great support, encouragement and patience through my all studies and during my Ph.D. so, Thank you very much for everything.

I would like to extend my deepest gratitude to my supervisor Professor Khaled Elleithy for his continues guidance, support and encouragement throughout my thesis. Above all, he always congratulated me on every improvement and accomplishment in my studies. I am very fortunate to have my supervisor giving me opportunities to travel and join several professional research events.

Also, I would like to express many thanks to my friends and colleagues at the University of Bridgeport at the Department of Computer Science and Engineering for the many hours of useful, intellectual and inspiring discussion.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER 1: INTRODUCTION

1.1 Motivation

Cryptography is the most fundamental element of computer and network security. Security services including confidentiality, authentication, and privacy depend on the techniques of cryptography. Communication security is a subfield that offers a private communication channel between a sender and a receiver. Also, it deters intruders from message content. Throughout history, cryptographic techniques have typically been broken sometime after being invented. In 1926, Vernam invented the one-time pad encryption technique [1], which is also called the Vernam cipher. The algorithm is based on symmetric encryption with a long secret key known to the sender and the receiver. Moreover, one-time pad encryption achieves perfect secrecy when the secret key is not reused. A few decades later, Shannon proved that one-time pad encryption is ideal and sufficient when the length of the secret key is as long as the plaintext [2]. However, distant parties need a secure method to share the long secret key. The security of current cryptographic techniques is based on hard-to-solve mathematical problems, but it is not secure in principle. Current algorithms can be adjusted to accommodate more computational power than that of available algorithms. Hence, a computer with significant power puts the current algorithms at risk. In the past few decades, quantum physics introduced a new type of cryptography. Bennett and Brassard were the first to propose secret key distribution using

the properties of quantum mechanics in 1984 [3]. Then, Ekert's idea in 1991 [4] was the trigger of quantum key distribution. As a result, quantum cryptography became an active research topic in theory and experiments. Ten years later, Peter Shor discovered that manipulating coherent quantum states makes it possible to factor large numbers [5]. Hence, factoring large numbers is a mathematical problem that is difficult to solve using classical computing, and public key cryptography such as RSA specifically depends on that problem. Therefore, the capabilities of quantum computing put current cryptographic techniques at risk.

The basic building block of quantum key distribution includes two distanced parties (traditionally known as Alice and Bob) cooperating to set up a secret key Figure 1.1. Both have access to insecure quantum and authenticated classical channels. Compromising the quantum channel is possible with no limit on the attacker (traditionally known as Eve) who obeys the laws of quantum physics. However, only eavesdropping is possible on the classical channel. Alice and Bob need to protect their quantum channel from Eve during data transmission. For this reason, they either form a secret key with high confidence or they abort the channel. The confidence is based on estimating the quantity of information Eve gained during the communication process. The concept of information leakage from eavesdropping is not available in the classical channels because it goes undetected. In contrast, quantum physics quantifies the information leakage in the quantum channel, making it possible to be detected.

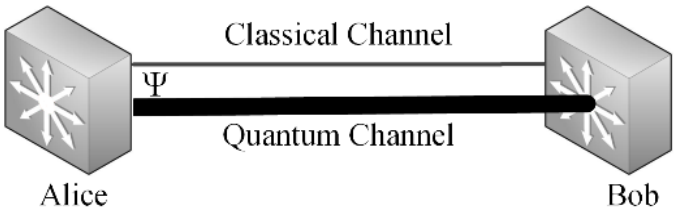

Figure 1.1 Building Block of QKD

Quantum computing has introduced new theories to information security; for instance, measuring the quantum bit (qubit) disturbs the original system. Unlike copying in classical signals, it is impossible to copy a qubit based on the no-cloning theorem because measurement affects the original system [6]. Another approach considers separated measurement on entangled states and Bell's inequalities for quantum security. Measurement on correlated qubits violates Bell's theorem, and it is impossible to prove that they were created in an earlier agreement. So, measurement did not occur before, and an eavesdropper cannot have prior information [4]. Therefore, quantum cryptography offers unconditional security because it depends on the principles of quantum physics without assuming power limitation on the eavesdroppers.

1.2 Domain and the Specific Problem

Quantum key distribution is the domain of this research. The specific problem we are investigating is finding a secure and efficient entanglement-assisted three-party quantum key distribution protocol between two untrusted to each other parties. Also, we investigate the problem of distributing entanglement in typical telecom metropolitan optical network. A centralized EPR source creates then distributes entanglement to users in different access networks. We need to create a dynamic network using reconfigurable

optical add/drop multiplexers to serve the entire network. Classical and quantum signals will be travelling in the same network.

1.3 Results and the Potential Contributions of the Proposed Research

Secure communication by teleporting an unknown quantum state from a sender to a receiver is known to consume two bits of classical communication, given that the sender and the receiver prior share an Einstein-Podolsky-Rosen (EPR) pair. Remote state preparation allows a known quantum state to a sender to be securely prepared at a remote receiver is using one bit of classical communication given that the parties prior shared an EPR pair. Therefore, in a network where every user is authenticated to a trusted authority, but not to each other, establishing a secret key between two users costs classical and entanglement bits. In this thesis we show how a three-party quantum secret key distribution protocol can be created using parity bits of the EPR pairs, controlled gates, and ancillary states [7]. It distributes a secret key of d qubits by means of $2d$ entangled pairs and, on average, d bits of classical communication.

Moreover, in this thesis we also study the architecture of metropolitan optical networks (MON) and how to distribute entanglement in a typical telecommunication infrastructure. We analyzed the MON architecture to allow simultaneous transmission of classical and quantum signals in the network and show a dynamic routing mechanism to serve the entire network [8]. The strong launch power of the classical signals impairs the weak quantum signals when they coexist in the same optical fiber. Raman scattering Stokes shift is the major physical impairment on the higher wavelength quantum signals which, caused by the lower wavelength classical signals. Therefore, we also studied the physical

impairments in the network to reduce the nonlinear effects and improve the quality of the signals. We showed an architecture where quantum and classical signals travel in the same optical fiber, but in different spectral bands. Also, we showed Raman Stokes-shift wavelength range and the peak power gain when simultaneous transmission of both signals occurs in the same optical fiber. Reducing the physical impairments increases the traveling distance of the signals and the number of the access networks in the MON.

CHAPTER 2: LITERATURE SURVEY

2.1 Introduction

The advancements of quantum mechanics in information processing, computing, communication, and cryptography make it an interesting research area. In quantum communication, quantum states play an important role because they carry the information in the quantum communication channels. Additionally, an interesting application of quantum information processing is quantum teleportation presented by Bennett et al [9]. It transmits an unknown quantum state using a quantum channel made of an Einstein-Podolsky-Rosen (EPR) pair and two classical bits of information. Subsequently, a variant of the quantum teleportation protocol called remote state preparation (RSP) was presented by Lo [10], Pati [11] and Bennett et al [12]. Remote state preparation transmits a quantum state known to the sender (Alice) but unknown to the receiver (Bob). For example, when Alice wishes to send a state to Bob, Alice performs a projective measurement on her qubit in the shared entanglement and then informs Bob of the result through an authenticated classical channel. Then, Bob uses the information received from Alice to reconstruct the state on his qubit in the shared entanglement. Remote state preparation is also known as teleportation of a known quantum state because it shares the same goal with the teleportation. One difference between remote state preparation and teleportation is the strong trade-off in remote state preparation between the required number of entanglement and classical bits. This trade-off results from the sender's prior knowledge of the state to be transmitted. The classical communication cost of remote state preparation is one

classical bit for each qubit, half of the required classical bits in teleportation. Therefore, remote state preparation became an active research area both theoretically and experimentally.

2.2 Two-Party Remote State Preparation Protocols

2.2.1 Equatorial

A generalization of quantum-communication complexity in [10] studies the cost of classical communication in quantum information processing and the major laws governing quantum information processing. It considers the communication cost in quanta as a natural generalization of quantum communication complexity. As a result, it breaks quantum teleportation into two processes. The first process consists of the pure state $\alpha|0\rangle + \beta|1\rangle$ at the sender Alice side. In addition, Alice and the receiver Bob share an entangled state such as $\alpha|00\rangle + \beta|11\rangle$. The second process will result in state $\alpha|0\rangle + \beta|1\rangle$ completely at Bob's location. Thus, the representation of each state involves one classical bit. Alice can help Bob to reconstruct a state known to her but unknown to him using classical communication if the state is chosen from some pre-agreed set. Alice helps Bob reconstruct the prepared state by sending only one classical bit. Remote state preparation is different from teleportation because Alice knows the precise state she wishes to transmit. Thus, the required classical cost in remote preparation is half of that required in teleportation. The minimum classical bit for remote preparation in [11] states that for a qubits chosen from the equator on a Bloch sphere, Alice can help Bob to prepare a state by sending one classical bit, provided that Alice and Bob share a maximally entangled pair. Alice completely knows the state she wishes to communicate with Bob. For example, Alice has

a pure state $|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle$ she wishes to transmit to Bob such that $|\Psi\rangle \in H = C^2$. And, in the pure state, the coefficients α and β are real and complex numbers, respectively. Instead of sending a physical quantum state or a huge amount of classical information, Alice can use a new method. Alice measures her entangled qubit by projecting it into one of the qubit basis [$|\Psi\rangle, |\Psi \perp\rangle$]. Then, performing a Von Neumann measurement will result in having Alice's state as the original input or its complement. After that, Alice informs Bob using one classical bit if he needs to keep his state or transform it to its orthogonal complement. Remote state preparation in [12] provides an asymptotic cost of classical communication. It shows that the asymptotic cost is one classical bit for each qubit, which is half of the classical cost in teleportation and gives the tradeoff between the components in remote state preparation, for instance, the tradeoff between the classical and the entangled bits. It reuses the entangled bits from Alice to Bob in the backward communication from Bob to Alice. This feature is possible in remote state preparation but not in quantum teleportation. Further, it introduces two types of channel capacities for noisy channels to communicate a known state to the sender with or without prior shared entanglement. The problem of transferring quantum states using a noiseless classical channel and prior shared entanglement channel is shown in [13]. It studies a situation where the sender has full knowledge of the target state. The proposed scheme shows a trade-off between superdense coding, data compression and remote state preparation techniques. And it gives a formula to calculate the trade-off of the date compression to evaluate the three techniques. It shows that they are optimal and achievable when incorporating two techniques.

2.2.2 Low-Entanglement

The low-entanglement remote state preparation in [14] introduces a new method to find the tradeoff between the classical bits and the entangled bits by utilizing classical information theory techniques. It is the optimal approach among the low-entanglement remote state preparation protocols because it uses classical messages followed by quantum teleportation. However, this protocol is based on teleportation and does not require back communication. Therefore, teleportation-based protocols are optimal among other low-entanglement schemes.

2.2.3 High-Entanglement

Remote-state preparation in higher dimensions and the parallelizable manifold S^{N-1} in [15] addresses remote state preparation in real Hilbert Space to generalize the result of Pati's protocol [11] in higher dimensions and proves that the implementation of remote state preparation can only be performed in real Hilbert space with 2, 4, and 8 dimensions. However, there are no dimensional restrictions for states prepared on the equator or the polar great circle on the Bloch sphere. The generalization of remote state preparation was provided to prepare an equatorial state of the form:

$$|\Psi\rangle = \sum_{\alpha=0}^{n-1} \frac{1}{\sqrt{n}} e^{i\theta_\alpha} |\alpha\rangle \tag{2.1}$$

By setting the value of $\theta = 0$, remote state preparation can be realized when the dimension is n. Alice performs the unitary transformation $U_A(|\Psi\rangle)$ on her particle in the shared entanglement $|\Phi^+\rangle_{AB}$:

$$U_A(|\Psi\rangle) \otimes I_B|\Phi\rangle_{AB} = \sum_{\alpha=0}^{n-1} \frac{1}{\sqrt{n}} |\Psi\rangle_\alpha \otimes |\Psi\rangle_\alpha \tag{2.2}$$

Alice measures her particle on the basis $\{|\Psi_\alpha\rangle\}_{\alpha=0}^{n-1}$ and then sends the result to Bob to perform U_α^{-1} to reconstruct $|\Psi\rangle$.

2.2.4 Noisy Entanglement

Remote preparation of pure states via noisy entanglement in [16] provides an experimental and general scheme. It remotely prepares the states using auxiliary qubit and controlled-not gate. Additionally, it provides remote state preparation with a depolarizing and dephasing decoherent. Therefore, it realizes remote state preparation dephasing channels in practice by performing the spontaneous parametric down conversion process in addition to utilizing single photon detectors and linear optics. As a result, they found that the experiments match the theoretical work.

2.2.5 Optimal

Optimal remote state preparation in [17] proves remote state preparation for a non-commuting mixed state. The protocol uses communications equal to Holevo information

$$S(\sum_i pi\rho i) - \sum_i piS(\rho i) \tag{2.3}$$

$$S(\rho) = -Tr(\rho \, log_2 \, \rho) \tag{2.4}$$

to transfer different ensembles of mixed states, where $S(\rho)$ is the von Neumann entropy. In classical information theory, the average bits of message compression equals to Shannon entropy $H = -\sum_i pi \log_2 pi$ for message i that has probability pi. To clarify, having H

bits for each message is adequate to reconstruct a sequence of messages. Alternatively, it is possible to obtain H bits from each message. Considering the quantum information theory, if we have density operator ρi with probability pi, it is possible to obtain similar analysis to Holevo information [18]–[20]. Therefore, it is possible to create classical communication equal to Holevo information. Consequently, reversing this operation makes remote states preparation possible using Holevo information. Thus, back-and-forth conversion between ensembles of mixed states and classical information is possible in a lossless way.

2.2.6 Oblivious and Non-Oblivious

Oblivious remote state preparation in [21] proposes a protocol similar to quantum teleportation. It is oblivious to the sender because the sender needs to provide a specimen of the state to the receiver without having full knowledge about the state being prepared. In contrast to the oblivious to the receiver protocol, which is similar to quantum teleportation, the receiver does not have any information about the state being prepared except the specimen. Consequently, the classical information required in this protocol is equivalent to the classical information required in quantum teleportation. The protocol in [22] provides a remote state preparation protocol without the oblivious condition to the receiver. It derives the necessary equations to prove that Bob's operations can be unitary transformations. Therefore, this protocol requires Alice to send two classical bits of information to Bob for each communicated qubit. Therefore, the classical information cost in this protocol is equal to the classical cost of quantum teleportation even when assuming it is oblivious to Bob.

2.2.7 Faithful

The faithful remote state preparation protocol in [23] uses finite classical bits and a non-maximally entangled state. The protocol remotely prepares an ensemble of quantum states by the minimum classical information by using prior shared non-maximally entangled pairs as the communication channel. Moreover, it provides all the ensembles in two-dimension cases, making it possible to communicate any pure state faithfully using the remote state preparation protocol. For example, using finite classical bits and prior shared non-maximal entanglement to prepare a state remotely. In contrast, it is not possible to achieve quantum teleportation by prior shared non-maximally entangled pairs.

2.2.8 Continuous Variable

Remote state preparation and teleportation in phase space [24] addresses the Wigner function to analyze continuous variable remote state preparation. It introduces a new remote state preparation scheme based on the squeezed state, and the participating parties share entangled twin beams. One beam has homodyne detection acting as the conditional source for the squeezed state. Additionally, it works in a noisy environment, especially when the homodyne efficiency is more than one-half. Moreover, state teleportation in the phase space works as the generalized conditional measurement and provides a way to measure degrading effects such as losses in the line, the amount of entanglement and sender efficiency. Continuous variable remote state preparation in [25] provides an exact and deterministic protocol with minimal classical communication. It proposes a method to prepare states of an ensemble described by infinitely real numbers such as a real function. Moreover, the protocol shows demonstrations using quadrature

measurement, optical phase measurement, and photon counting and shifting. So, the classical communication cost is one classical bit and one maximally entangled bit.

2.2.9 Multi-State

The protocol in [26] provides a scheme to communicate a two-particle qubit using remote state preparation.

$$|\varphi_{in}\rangle = \alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle \tag{2.5}$$

It needs two non-maximally entangled pairs as a quantum channel.

$$|\Psi\rangle = u|01\rangle - v|10\rangle \tag{2.6}$$

$$|\Phi\rangle = w|00\rangle - z|11\rangle \tag{2.7}$$

And it gives the effect of environment noise on the states and defines the effect on state fidelities using three channels. Also, it finds that the output fidelities of states with basis $\{|01\rangle, |10\rangle\}$ are higher than a state with basis $\{|00\rangle, |11\rangle\}$. Remote state preparation of a three-particle state in [27] remotely prepares three-qubit GHZ states using a quantum channel of two and three entangled pairs. In particular, the two-qubit channel is maximally entangled, and the three-qubit channel is non-maximally entangled. Therefore, the success probability when suing forward classical information is one-half and costs on average one-half classical bit. However, for special states, the success probability became a unit, but it costs one more classical bit on average. Remote preparation of a class of three-qubit GHZ state:

$$|u\rangle = \alpha|000\rangle + \beta|111\rangle + \gamma|001\rangle + \delta|110\rangle \tag{2.8}$$

States in [28] communicate the state using three two-particle maximally entangled pairs as the quantum channel.

$$|\Psi\rangle_{123456} = |\Phi^+\rangle_{12} + |\Phi^+\rangle_{34} + |\Phi^+\rangle_{56} \tag{2.9}$$

Additionally, it provides the probability of success and the cost of the classical bits. The receiver uses unitary operations to reconstruct the prepared state with a success probability of one-fourth. However, for special states, the success probability reaches one-half or a unit when consuming extra classical bits. Remote preparation of a two-particle entangled state in [29] prepares a two-dimensional two-particle entangled qubit. It communicates the state using two-qubit entangled pairs as the communication channel and provides a generalization for entanglement in higher-dimensions. The protocol prepares equatorial state with a unit probability by using two maximally entangled pairs, two classical bits of information, and two-particle projective measurements. However, if the quantum channel is two non-maximally entangled pairs, then realizing the two-dimensional two-particle entangled state will be probabilistic. The scheme in [30] prepares four-particle entangled W states. The scheme provides a probabilistic method to prepare a remotely four-particle W state. It uses a quantum channel and consists of four partially entangled pairs. Moreover, the sender performs projective measurement on the quantum channel and then sends the result to the receiver through the classical channel. Based on the sender result, the receiver performs a specific unitary operation. As a result, the receiver will successfully realize the prepared states with high probability. Nevertheless, achieving a unit probability is possible when considering some special cases. The cost of this scheme is one classical bit and entanglement of a four-particle state to achieve a success probability of one-fourth. The protocol to prepare arbitrary two- and three-qubit states via the χ state is presented in [31].

The protocol constructs measurement bases using a Routh-Hurwitz matrix to communicate arbitrary two-qubit and three-qubit states remote using an entangled χ state as the quantum channel.

$$|\chi\rangle_{1234} = \frac{1}{2}(00\rangle|\varphi^-\rangle - |01\rangle|\psi^-\rangle + |10\rangle|\psi^+\rangle + |11\rangle|\varphi^+\rangle)_{1234} \quad (2.10)$$

The success probability of this scheme is as high as one and one-half for real and complex coefficients, respectively. And the classical cost is four and six bits for real and complex coefficients of the channel, respectively. However, a special type of ensemble with complex coefficients can achieve unit success probability at the cost of more classical bits.

2.3 Three-Party Remote State Preparation Protocols

2.3.1 Joint

Joint remote state preparation of arbitrary qubits is presented in [32]. It introduces a probabilistic scheme of remote state preparation to transfer a general two-qubit state.

$$|\Phi\rangle = \lambda_0|00\rangle + \lambda_1 e^{i\theta_1}|01\rangle + \lambda_2 e^{i\theta_2}|10\rangle + \lambda_3 e^{i\theta_3}|11\rangle \quad (2.11)$$

The scheme allows senders to remotely prepare a state to a receiver. In addition, the parities will use a quantum channel made of multipartite entangled GHZ states. The scheme is extendable to deliver an arbitrary three-qubit state. It requires two tripartite GHZ states and three classical bits to achieve a success probability of one-fourth. However, it is possible to achieve deterministic results by consuming more classical bits. The joint remote preparation of an arbitrary three-qubit state in [33] introduces a method for two senders to jointly prepare a remotely three-qubit state containing complex coefficients. In addition,

the method uses a permutation group to improve the preparation success rate by preparing three-qubit states with real coefficients and different measurement bases. Furthermore, the protocol is extendable to serving multi-senders sharing a state coefficient. The scheme has a success probability of one-half for preparing a complex coefficient three-qubit state and μ^2 for a real coefficient state. And they have a classical cost of $\log_2 13$ and $\log_2 9$ for the complex and real coefficients, respectively. Joint remote preparation of an arbitrary three-qubit state via EPR-type pairs are presented in [33]. This scheme provides a realization for remote state preparation. It prepares an arbitrary three-qubit state using six Einstein-Podolsky-Rosen pairs as a quantum channel. In addition, it has an extension to prepare the three-qubit state. Further, the sender chooses the optimal measurement bases, so the receiver needs to use the appropriate ancilla-assisted for the unitary transformation. Moreover, the scheme applies to the case where the entanglement and the target state coefficients are complex. The success of the scheme depends on the smaller coefficient of the entangled pairs making the scheme secure and faithful for quantum communication.

Joint remote state preparation of an arbitrary two-qubit state with a six-qubit state is presented in [32]. This scheme provides a novel probabilistic remote state preparation to remotely prepare a general two-qubit state. Also, it allows remote senders to prepare a two-qubit state for one receiver using a quantum channel that consists of a cluster of six-qubit states. The two senders perform projective measurements on their parts of the cluster state and inform the receiver of the results of their measurements. Then, the receiver performs a unitary transformation to reconstruct the expected state. The success probability of the general case is one-fourth. However, for special states and bases, the success probability ranges from one-fifth to a unit. The cost of this scheme is a cluster of six-state and four

classical bits. Probabilistic joint remote preparation of a two-particle high-dimensional equatorial state is presented in [34]. This protocol provides joint remote state preparation of an arbitrary equatorial two-qubit state in high-dimension.

$$|\Psi\rangle = \sum_{n=0}^{2} \sum_{m=0}^{2} Z_{mm} |mn\rangle \tag{2.12}$$

It allows two separated senders to help a receiver to reconstruct the state. The three parties share two non-maximal entangled states in three dimensions as a quantum channel. Senders need to perform a projective measurement on their shared qubits and inform the receiver of their result to perform a unitary transformation. The success probability of this scheme depends on the coefficients of the quantum channel. Therefore, this scheme costs two entangled bits and $4 \log_2 3$ classical bits. Joint remote state preparation for two-qubit equatorial states are presented in [35]. It transfers a two-qubit equatorial pure state using three-party joint remote state preparation. The quantum channel of this protocol consists of two GHZ maximally entangled states

$$|\Psi\rangle = |\psi\rangle_{135} \otimes |\psi\rangle_{246} \tag{2.13}$$

and involves a unitary transformation and projective measurement. The success probability of this protocol is one-fourth, and it costs four classical bits of information. The Joint remote preparation of an arbitrary five-qubit Brown state in [36] provides a novel deterministic protocol. This protocol remotely prepares a five-qubit Brown state using four non-maximally entangled GHZ states as quantum channels. This scheme has a success probability of up to one. For comparison, the scheme is extended using non-maximal three and four entangled qubit states as the quantum channel and applying both methods to

prepare and reconstruct the target states. The first scheme provides better success probability and has a classical cost of seven bits.

2.3.2 Tripartite Entanglement

Remote preparation of a multipartite pure state in [37] remotely prepares a pure quantum state using prior shared tripartite entanglement. It costs one classical bit and one tripartite entangled state. However, the tripartite entanglement source requires a cavity quantum electrodynamics technique [38]. Consequently, the participating users will share a pure qubit when consuming one classical bit. This protocol prepares an instance of a quantum state remotely [39]. It prepares an equatorial state at two locations in one-shot and requires one prior entangled tripartite state

$$|\phi_0\rangle = \frac{1}{\sqrt{2}}(|0\rangle_A|0\rangle_B|0\rangle_C + \frac{1}{2}|1\rangle_A|0\rangle_B|0\rangle_C + \frac{1}{2}|1\rangle_A|1\rangle_B|0\rangle_C \quad (2.14)$$

$$|\phi_1\rangle = \frac{1}{\sqrt{2}}(|1\rangle_A|1\rangle_B|1\rangle_C + \frac{1}{2}|0\rangle_A|0\rangle_B|1\rangle_C + \frac{1}{2}|0\rangle_A|1\rangle_B|0\rangle_C \quad (2.15)$$

and one classical bit to communicate the state to two receivers. Also, it provides a trade-off between entanglement bits and the fidelity of the states. Moreover, the protocol can be extended to prepare two instances of quantum state at one location using one prior entangled pair and one classical bit of information. Classical communication cost and remote preparation of a multi-qubit with three parties are presented in [40]. The protocol is probabilistic and shares a multi-qubit state between three parties. This protocol uses a tripartite partial entangled GHZ state as a quantum channel. Moreover, the scheme prepares general and special states chosen from the equator on the great circle of the Bloch sphere. This scheme has a success probability of one-half and one for general and special qubits,

respectively. The classical communication cost for the general case is 1.5 bits and three bits for the special case. Remote preparation of an entangled two-qubit state with three parties is presented in [41]. This probabilistic protocol remotely prepares two-qubit entangled states between three parties. The sender shares a state with one of two participating receivers. In addition, it requires two and three partially entangled states as quantum channels. Also, it defines the success probabilities for general and special cases. The cost of the classical for the general state is 2.5 bits, and the success probability is one-half. However, the classical cost for special states is five bits, and the success probability is a unit.

2.3.3 Controlled

The controlled remote state preparation scheme [42] remotely prepares a quantum state controlled by different parties. It uses quantum key distribution to control the remotely prepared states. In addition, reconstruction of the state has a success probability of one-half. However, the success probability reaches a unit when all parties participate. Further, this scheme was the first controlled remote state preparation. It also transfers a group of multi-qubit states using the bell basis. Consider a scenario where Alice wishes to communicate a state to Bob and needs Charlie to control the state. This task requires Alice and Charlie to have one prior shared classical information bit. After that, Alice measures her entangled states and obtains one bit, which shows whether Bob's state is correct. Alice encrypts her measurement result bit in the C-NOT gate using the shared bit with Charlie and sends the encrypted bit to Bob. Therefore, for Bob to successfully recover the correct bit, he needs to communicate with Charlie to get the shared bit with Alice. Upon receiving

the secret bit, Bob can perform the C-NOT gate and find out if the state in his possession is correct or if he needs to apply a unitary transformation. Multiparty-controlled remote state preparation of a two-particle state [43] introduces a scheme to prepare an entangled two-particle qubit remotely by two non-maximally GHZ states

$$|\psi\rangle_{ABC} = a|000\rangle_{ABC} + b|111\rangle_{ABC} \tag{2.16}$$

$$|\psi\rangle_{A'B'C'} = c|000\rangle_{A'B'C'} + d|111\rangle_{A'B'C'} \tag{2.17}$$

as the quantum channel. In addition, it allows one sender to prepare a qubit for specific receivers. Realizing the prepared qubit is certain using projective measurement and the controlling particle. However, the coefficients of the channel states play a major role in the success probability. This scheme has a success probability of one-half and it requires six classical bits.

2.3.4 Multi-qubit

The multiparty remote state preparation protocol in [44] solves the problem of transmitting a shared state between two parties and a multiparty to a receiver. It provides two protocols. The first protocol considers sharing a state between two parties. The second protocol is the generalization to consider N parties. In the first protocol, the senders and the receiver share a non-maximally entangled GHZ state, where the first senders perform a projective measurement on the shared qubit and transfer the classical result to the second sender. Then, the second sender performs a projective measurement on their qubit based on the classical result of the first sender. After that, the second sender sends the result of the classical measurement to the receiver. Finally, based on the received classical information, the receiver performs a unitary transformation on the shared qubit to obtain

the intended state. For multiparty state sharing, it assumes that all the parties share a multiparty entangled state. Therefore, this protocol requires an $N+1$ particle GHZ entangled state. The senders share particles 1 to N, and the receivers share the particle $N+1$. Following the same steps in the two-party protocol, the senders end up preparing the shared state at the receiver's location. Finally, the receiver performs a local operation and unitary transformation to build the target state.

2.3.5 Entangled State

Remote state preparation of an entangled state as presented in [45] is a protocol to communicate a two-particle entangled state by a three-particle GHZ state quantum channel. In addition, it provides generalization for specific entangled multi-particle states. The cost of this protocol is one classical bit and one three-particle entangled GHZ State. Hence, preparing N entangled states using a GHZ state entails one classical bit and one projective measurement, as the number of classical bits does not increase when increasing the number of particles. The success probability for a general state is one-half; however, for some special states, it is a unit. Moreover, the three-party QKD scheme in [46] distributes a general qubit state to two users using two entangled states as the quantum channel and three bits of classical communication. And the required operations are one projective measurement, one Bell state measurement, and three unitary operations.

2.3.6 Dark States

This protocol is the generalization for multiparty remote state preparation [47]. The goal of this protocol is to allow a sender to prepare quantum states remotely at different

locations for multiple receivers. It requires prior entanglement states, four-particle dark state

$$|\Psi\rangle_{1234} = \frac{1}{2}[|0011\rangle + |1100\rangle - |0110\rangle - |1001\rangle] \quad (2.18)$$

local operations, and an authenticated classical channel. Further, it is also generalized for high-dimension states. For instance, the generalization covers qubits, qutrits, and qudits. More importantly, this protocol uses multi-particle measurement and dark states. The cost of this protocol is $log_2 d$ classical and four-particle dark entanglement bits for each participant.

2.3.7 W State

Deterministic remote preparation of an arbitrary W class state with multiparty in [48]. The W state has the form:

$$|W\rangle = a_1|001\rangle + a_2|010\rangle + a_3|100\rangle + a_4|111\rangle \quad (2.19)$$

This protocol uses remote state preparation to remotely prepare a deterministic state from a sender in one location to one of many separated receivers. The protocol assumes there is no prior entanglement shared between the sender and the receiver. Therefore, it applies entanglement transformation to establish the preparation process. The sender will deterministically prepare the intended state at the receiver's location. The quantum channel in this scheme consists of two four-particle GHZ states. In addition, the sender will use a real spectra measurement basis in the preparation process. Moreover, it is possible to extend the scheme to a server multiparty setup. The cost of this scheme is two four-particle GHZ states and six classical bits to achieve unit success probability.

2.4 Four-Party Remote State Preparation Protocols

2.4.1 Joint

Joint remote state preparation protocol to remotely prepare qubits using W state in [49]. It solves the problem of sharing a single-qubit with three parties by using a three-atom W state as a quantum channel, as it takes advantage of atom stability to transfer the states. Based on prior knowledge of the target qubit, senders must perform operations on their qubits. The success probability of preparing the target state at the receiver's location depends on the original method of creating that state. Therefore, reconstructing the target state depends on the received classical information and the preparation method. This protocol costs two classical bits and a three-entangled-atoms W state. The joint remote state preparation protocol in [50] allows multi-senders to prepare many states for two-receivers. The senders prepare many qubits for the receivers, allowing them to reconstruct the target state simultaneously using multiple composite GHZ states as the communication channel. In addition, it allows states with real and complex coefficients. Therefore, the classical cost in this protocol is $6N$ bits, and its success probability is $(1/4)Exp(N-1)$, where N is the number of senders.

2.5 Comparison and Analysis of Remote State Preparation Protocols

Comparison between remote state preparation protocols in Table 2.1. We divide the table into two-party, three-party, and four-party protocols. We will focus on the relationship between the qubits, entangled bits, and classical bits under different entanglement channels and the type of communicated states.

Table 2.1 Comparison between RSP protocols

Article	Q	E	C	Ch. Entanglement	State Type	Parties	S	R	Deter/Prob	Success	L.O.	S.M	R.M
[10]	1	1	1	Maximally	Special	2	1	1	Deterministic	1	σ_z	Projective	Unitary
[11]	1	1	1	Maximally	Special	2	1	1	Deterministic	1	Pauli	Projective	Unitary
[12]	1	1	1	Maximally	Special	2	1	1	Deterministic	1	σ_z	Projective	Unitary
[14]	1	<1	2	Maximally	Special	2	1	1	Deterministic	1	Pauli	Bell	Unitary
[15]	1	1	1	Maximally	Special	2	1	1	Deterministic	1	Pauli	Projective	Unitary
[17]	1	1	1	Maximally	Mixed	2	1	1	Probabilistic	~1	Pauli	POVM	Unitary
[21]	1	1	2	Maximally	Mixed	2	1	1	Deterministic	1	Pauli	POVM	Unitary
[22]	1	1	2	Maximally	Mixed	2	1	1	Deterministic	1	Pauli	POVM	Unitary
[13]	1	1	1	Maximally	Special	2	1	1	Deterministic	1	Pauli	Projective	Unitary
[23]	1	1	2	Non-Maximally	Special	2	1	1	Deterministic	1	Pauli	POVM	Unitary
[24]	1	1	1	Maximally	Special	2	1	1	Deterministic	1	Pauli	POVM	Unitary
[25]	1	1	1	Maximally	Special	2	1	1	Deterministic	1	Phase space	Quadrature	Displacement
[16]	1	1	1	Maximally	Special	2	1	1	Deterministic	1	$\sigma_z, i\sigma_z$	Projective	Unitary
[51]	1	1	1	Maximally	Special	2	1	1	Deterministic	1	σ_z	Projective	Unitary
[52]	1	1	1	Maximally	Special	2	1	1	Deterministic	1	σ_z	Projective	Unitary
[26]	2	2	2	Non-Maximally	Mixed	2	1	1	Probabilistic	1/2	Pauli	Projective	Post-Selection
[27]	3	2	.5	Maximally	GHZ	2	1	1	Probabilistic	1/2	Pauli	Projective	Unitary
[28]	3	3	.25	Maximally	Mixed	2	1	1	Probabilistic	1/4	Pauli	Projective	Unitary
[29]	2	2	2	Maximally	Special	2	1	1	Deterministic	1	Pauli	Projective	Unitary
[30]	4	4	1	Non-Maximally	W	2	1	1	Probabilistic	1/4	Pauli	Projective	Unitary
[31]	2	1	4	χ State	Special	2	1	1	Deterministic	1	Pauli	Projective	Unitary
[32]	6	2	3	Maximally GHZ	Special	3	2	1	Probabilistic	1/4	Pauli	Projective	Unitary
[37]	1	1	2	Maximally Tripartite	Special	3	1	2	Deterministic	1	σ_z	Projective	Unitary
[39]	1	2	2	Maximally Tripartite	Special	3	1	2	Deterministic	1	σ_z	Projective	Unitary
[42]	1	1	2	Maximally	Mixed	3	2	1	Probabilistic	1/2	σ_z	Projective	Unitary
[40]	1	1	3	Maximally GHZ	Special	3	1	2	Deterministic	1	σ_z	Projective	Unitary
[41]	2	5	2.5	Non-Maximally	Mixed	3	1	2	Probabilistic	1/2	Pauli	Projective	Unitary
[33]	3	3	<3.8	Maximally GHZ	Mixed	3	2	1	Probabilistic	1/2	Pauli	Projective	Unitary
[33]	3	3	4	Non-Maximally	Mixed	3	2	1	Probabilistic	1/8	Pauli	Projective	Unitary
[44]	1	1	2	Non-Maximally GHZ	Special	3	2	1	Probabilistic	1/2	σ_x	Projective	Projective
[45]	2	3	1	Maximally GHZ	Special	3	2	1	Probabilistic	1/2	Pauli	Projective	Unitary
[46]	2	2	3	Maximally GHZ	Special	3	1	2	Deterministic	1	Pauli	Projective	Unitary
[47]	1	2	2	Dark State	Special	3	1	2	Deterministic	1	$i\sigma_z$	Projective	Unitary
[48]	3	2	6	Maximally GHZ 4-P	W	3	2	1	Deterministic	1	CNOT	Projective	Unitary
[32]	2	1	4	Cluster State 6-P	Mixed	3	2	1	Probabilistic	1/4	$\sigma_z \otimes \sigma_z$	Projective	Unitary
[33]	2	2	<6.4	Maximally GHZ	Mixed	3	2	1	Deterministic	1	Pauli	Projective	Unitary
[43]	2	2	6	Non-Maximally GHZ	Special	3	1	2	Probabilistic	1/2	Pauli	Projective	Unitary
[35]	2	2	4	Maximally GHZ	Special	3	2	1	Probabilistic	1/2	Pauli	Projective	Unitary
[36]	5	4	7	Maximally GHZ 4-P	Brown State	3	2	1	Deterministic	1	Pauli	Projective	Unitary
[49]	1	1	2	Maximally W	Special	4	3	1	Deterministic	1	Pauli	Projective	Unitary
[50]	2	1	12	Composite GHZ 4-P	Mixed	4	2	2	Probabilistic	1/4	Pauli	Projective	Unitary

Q=No. of qubits, E=No. Entangled bits, C=No. classical bits, S=No. of senders, R=No. of receivers, L.O=Local operations, S.M=Sender measurement, R.M=Receiver measurement, Special= Pre-agreed distribution, OB= Oblivious

Many variables affect the required classical communication of each protocol such as the number of ebits and the type of the state to be communicated. In [10]–[13], [15], [16], [24], [25], [29], [31], [51]–[53], the cost of the classical communication to transmit one qubit is one cbit and ebit. These protocols use the common elements of the RSP protocol, which are maximal entanglement and a special set of states. In [14], the

communication cost is two cbits to transmit one special qubit in a deterministic fashion. The extra cbit is required because low-entanglement was used in this protocol. The RSP in [17] consumes one classical bit and one ebit for each qubit when transmitting a general state but a probabilistic success rate. However, the algorithms in [21], [22] achieve deterministic success probability transmitting a general state and consuming one additional classical bit. Using a non-maximally entangled channel in [23] makes it possible to send one special qubit in a deterministic fashion using one ebit and two cbits. In [26], a non-maximally entangled channel transmits one general qubit at the cost of one ebit. Thus, the success probability of this protocol is one-half. The transmission of a three-qubit GHZ state in [27] costs two maximally entangled ebits and one-half cbit. The low amount of the classical information reduces the success probability to one-half. Similarly, the RSP in [28] sends three general states using a three-qubit maximally entangled channel and one-fourth cbit, resulting in further reduction in success probability of one-fourth. RSP or a four-qubit W special state in [30] requires four-ebit channels and one cbit. The non-maximal entangled channel and the low amount of classical communication makes this protocol probabilistic with a success rate of one-fourth. Increasing the classical communication helps in reducing the amount of ebits [31]. The transfer of two special qubits deterministically needs one maximally entangled ebit and four cbits. The protocol in [32], [45] transmits six qubits using two maximal ebits and three cbits. The reduction in classical communication results in probabilistic success of one-fourth and one-half. The transmission of a general one-qubit state in [42] by one maximally ebit and two cbits gave a success probability of one-half. The classical communication likewise positively affected the success probability in [33], [41], [43]. The special qubits in [36], [37], [40], [46], [48],

[49] can be transmitted deterministically because the cbits are the same or larger than the qubits. In [33], the non-maximal entanglement and the transmission of a general state reduces the success probability to one-eighth. However, the RSP in [44] showed better success because of the increase in the cbits compared to the qubits. Transmitting a general state in [32], [50] reduced the success probability in both protocols to one-fourth even when consuming more cbits.

CHAPTER 3: RESEARCH PLAN

3.1 Introduction

In this chapter, we study quantum cryptography in network communications for secret key distribution, specifically, the security and efficacy of entanglement-assisted three-party quantum key distribution. Using the formal methodological approach, we study how the entanglement-assisted quantum key distribution protocols consume the communication resource. Then, we create a three-party quantum key distribution protocol to establish secret keys between two users unauthenticated to each other. The parity bits of the shared EPR pairs are used by quantum controlled gates and ancillary states to reduce the classical bit communication. We show that the parity bits and the ancillary states offer a secure communication channel and reduce the classical communication consumption in the key distribution process. Any action from the attacker Eve over the channel presents noise, which can be unambiguously detected. Also, using privacy amplification passive leakage is eliminated. The distribution process between the parties offers secure key distribution and with efficient classical communication.

3.2 Preliminaries of Quantum Computing

3.2.1 Quantum Bits

Quantum computing takes the advantages of the laws of quantum mechanics to efficiently solve the difficult problems in classical computing. The bit is the fundamental unit in classical computing to represent and store data. However, the name of the same unit

in quantum computing is called a qubit. The difference between a bit and qubit is that a bit represents one of two different disjointed states such as a signal as high or low, a switch as on or off or a logical value as true or false. However, a qubit can represent one state or two states simultaneously; for example, a switch can be represented as being on and off and a logical value can be represented as being true and false at the same time. The notation of one qubit is $|0\rangle$ for bit '0' and $|1\rangle$ for bit '1'. A qubit can be found in both states $|0\rangle$ and $|1\rangle$. Such a state is called a superposition, and it can be represented as a linear combination of both stats as:

$$|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle \tag{3.1}$$

The coefficients α and the coefficient β are complex numbers in C^n, and the states $|0\rangle$ and $|1\rangle$ are an orthonormal basis in two-dimensional vector space. The determination of bit and qubit values in classical and quantum computers are different. For instance, we can easily examine a classical bit and determine if it is in state '0' or '1'. However, in qubits, we examine the coefficients α and β instead. Moreover, measuring a qubit results in either state $|0\rangle$ with probability of $|\alpha|^2$ or $|1\rangle$ with probability of $|\beta|^2$ where:

$$|\alpha|^2 + |\beta|^2 = 1 \tag{3.2}$$

Having both probabilities sum to one geometrically indicates that the qubit state must be normalized to length one in the two-dimensional vector space.

Two qubits in quantum systems can be represented by four states using the classical bit 00, 01, 10, 11. On the other hand, two qubits can be represented by four basis states denoted by $|00\rangle$, $|01\rangle$, $|10\rangle$, $|11\rangle$. Moreover, the two qubits can also be in a superposition

by forming a linear combination of states with their complex coefficient, which is often called an amplitude.

$$|\Psi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle \quad (3.3)$$

After the measurement of this multi-qubit state, the result will be similar to a system with only one qubit. For instance, the probability of having one of the four states can be donated by $|\alpha_x|^2$.

3.2.2 Quantum Gates

Classical systems depend on the wires and the logic gates in the digital circuits to carry and manipulate the information. For instance, the NOT gate in classical systems performs a specific operation, which is manipulating the stats '0' and '1' by interchanging their values in which they the state '0' becomes '1' and the state '1' becomes '0'. Similarly, the NOT gate in quantum systems interchange the state $|0\rangle$ to $|1\rangle$ and the state $|1\rangle$ to $|0\rangle$.

$$\alpha|0\rangle + \beta|1\rangle \longrightarrow \text{NOT} \longrightarrow \alpha|1\rangle + \beta|0\rangle \quad (3.4)$$

Moreover, another convenient way to represent quantum gates is in matrix form. For instance, quantum gates $I, X,$ and H, which represent the Identity, NOT and Hadamard gates, respectively, can be represented in term of matrices as follows:

$$\text{I} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \quad \text{X} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \quad \text{H} = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \quad (3.5)$$

3.2.3 Quantum Teleportation Overview

Quantum teleportation [9] is the technique of moving an unknown quantum state from a sender to a distance receiver. It faithfully communicates a quantum state without a

physical quantum communication medium. Quantum teleportation does not conflict with the no-cloning theorem that prohibits copying an arbitrary qubit [6]. The target states are destroyed in the process of quantum teleportation. However, the receiver will have the necessary quantum information to reconstruct the target qubit. Accomplishing this technique requires the communicating parties to share quantum resources beforehand. Specifically, the sender and the receiver need to share a member of the maximally entangled state known as Bell states, which are also called EPR (Einstein-Podolsky-Rosen) pairs. Bell states consist of two entangled qubits in a non-canonical basis, such as follows:

$$\left\{\frac{(|0\rangle + |1\rangle)}{\sqrt{2}}, \frac{(|0\rangle - |1\rangle)}{\sqrt{2}}\right\} \tag{3.6}$$

Creating Bell states requires a circuit containing Hadamard and CNOT gates. The circuit takes two inputs and maps them to one of the Bell states. For example, having $|00\rangle$ as an input and then applying Hadamard followed by CNOT gates will output $(|0\rangle + |1\rangle)|0\rangle/\sqrt{2}$ and then $(|00\rangle + |11\rangle)/\sqrt{2}$, respectively. Hence, a combination of two input bits will create one of the maximally entangled pairs $\{|\Phi^{\pm}\rangle, |\Psi^{\pm}\rangle\}$.

$$|\beta_{00}\rangle = |\Phi^{+}\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}} \tag{3.7}$$

$$|\beta_{01}\rangle = |\Psi^{+}\rangle = \frac{|01\rangle + |10\rangle}{\sqrt{2}} \tag{3.8}$$

$$|\beta_{10}\rangle = |\Phi^{-}\rangle = \frac{|00\rangle - |11\rangle}{\sqrt{2}} \tag{3.9}$$

$$|\beta_{11}\rangle = |\Psi^{-}\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}} \tag{3.10}$$

Consider a scenario where Alice and Bob share a member of a maximally entangled quantum state. For example, let us consider that Alice and Bob share the entangled state:

$$|\Phi^+\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}} \tag{3.11}$$

And Alice has an arbitrary unknown quantum state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ that she wishes to transmit to Bob. The initial teleportation process starts with $(|\psi\rangle \otimes |\Phi^+\rangle)$, where Alice has the first two qubits and Bob has the third. Then, Alice applies $(U_{CNOT} \otimes I)$, where the first qubit in her possession is the control qubit and the second qubit is the target. Following, Alice applies the Hadamard gate on the first qubit, so the state of the system becomes $(U_H \otimes I \otimes I)$. Further, the result of the Alice measurement operation on her qubits collapses all the states into one state of $|00\rangle, |01\rangle, |10\rangle \, or \, |11\rangle$ with equal probability of one-fourth. Hence, the Alice measurement destroyed the initial state $|\psi\rangle$. Accordingly, the state of Bob's qubit will depend on the result of Alice's measurement as follows:

$$|00\rangle : |\psi_{00}\rangle = |\Phi^+\rangle \, \frac{\alpha|0\rangle + \beta|1\rangle}{2} \tag{3.12}$$

$$|01\rangle : |\psi_{01}\rangle = |\Psi^+\rangle \frac{\alpha|1\rangle + \beta|0\rangle}{2} \tag{3.13}$$

$$|10\rangle : |\psi_{10}\rangle = |\Phi^-\rangle \frac{\alpha|0\rangle - \beta|1\rangle}{2} \tag{3.14}$$

$$|11\rangle : |\psi_{11}\rangle = |\Psi^-\rangle \frac{\alpha|1\rangle - \beta|0\rangle}{2} \tag{3.15}$$

Now, Alice sends the result of the measurement to Bob using the classical channel. Then, the classical information received from Alice is used to apply the appropriate unitary transformation on the shared qubit to recover the target state $|\psi\rangle$. The received classical bits will inform Bob if he needs to apply the $I, X, Z\ or\ Y$ gates.

$$\begin{aligned} \mathrm{U}_{00} &= \mathrm{I} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix},\ \mathrm{U}_{01} = \mathrm{X} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \\ \mathrm{U}_{10} &= \mathrm{Z} = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \mathrm{U}_{11} = \mathrm{Y} = \begin{bmatrix} 0 & -\mathrm{i} \\ \mathrm{i} & 0 \end{bmatrix} \end{aligned} \tag{3.16}$$

$$|00\rangle : \ \mathrm{I}(\alpha|0\rangle + \beta|1\rangle) = \alpha|0\rangle + \beta|1\rangle \tag{3.17}$$

$$|01\rangle : \ \mathrm{X}(\alpha|1\rangle + \beta|0\rangle) = \alpha|0\rangle + \beta|1\rangle \tag{3.18}$$

$$|10\rangle : \ \mathrm{Z}(\alpha|0\rangle - \beta|1\rangle) = \alpha|0\rangle + \beta|1\rangle \tag{3.19}$$

$$|11\rangle : \ \mathrm{Y}(\alpha|1\rangle - \beta|0\rangle) = \alpha|0\rangle + \beta|1\rangle \tag{3.20}$$

Applying the proper unitary gate by Bob results in having an identical state of Alice's unknown initial state. The cost of quantum teleportation to transmit an arbitrary unknown quantum state is one maximally entangled pair as a quantum channel and two bits of classical information. The circuit of quantum teleportation is depicted in Figure 3.1.

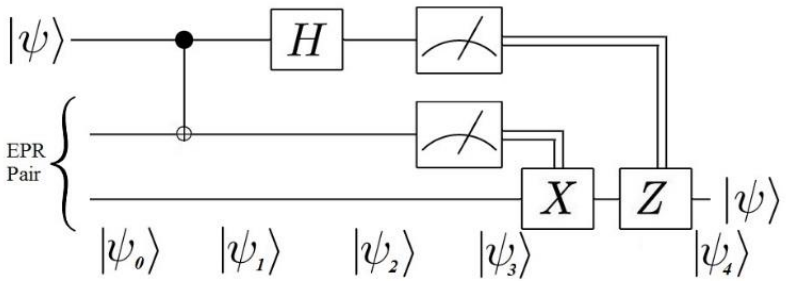

Figure 3.1 Quantum teleportation circuit

3.2.4 Remote State Preparation Overview

The concept of remote state preparation (RSP) [10]–[13] is similar to quantum state teleportation. In remote state preparation, the sender Alice helps the distant receiver Bob to reconstruct a quantum state. However, unlike quantum teleportation in remote state preparation, Alice knows exactly the state she wishes to communicate with Bob. For this reason, teleportation of the known quantum state is another description of remote state preparation. In addition, remote state preparation requires a single particle Von Neumann measurement instead of Bell measurement as in teleportation. Moreover, in remote state preparation, the target state Alice knows and wishes to communicate with Bob has no major effect in the process besides being known to Alice. However, achieving the expected performance requires states chosen from the special ensemble, for instance, choosing qubits from the equator or the polar line on the Bloch sphere. This is providing that Alice and Bob need to be sharing a maximally entangled pair and have access to an authenticated classical channel. To illustrate, suppose Alice has a pure state in the form:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \tag{3.21}$$

In addition, $|\psi\rangle \in H = C^2$, where α and β are real and complex numbers, respectively. In particular, the coefficients α and β have the form:

$$\alpha = \cos\frac{\theta}{2} \ , \qquad \beta = \sin\frac{\theta^{i\varphi}}{2} \tag{3.22}$$

where both θ and φ are real numbers. Hence, the location of the state is on the surface of a sphere S^2. Additionally, Alice and Bob must be sharing maximally entangled state $\{|\Phi^{\pm}\rangle, |\Psi^{\pm}\rangle\}$. Let us consider a scenario where the shared entanglement is the two-particle singlet state $\{|\Psi^{-}\rangle\}$. The singlet state has a total spin of zero. Therefore, if Alice measures her particle and finds it in a specific a state, Bob's particle will necessarily be antipodal to the result of Alice's particle. In other words, the states of Alice and Bob measurements will necessarily be orthogonal. For example, if Alice and Bob share a singlet state and the first particle (A) belongs to Alice and the second particle (B) belongs to Bob as follows:

$$|\Psi^{-}\rangle_{\mathrm{AB}} = \frac{|0\rangle_{\mathrm{A}}|1\rangle_{\mathrm{B}} - |1\rangle_{\mathrm{A}}|0\rangle_{\mathrm{B}}}{\sqrt{2}} \tag{3.23}$$

Alice knows the qubit she wishes to communicate with Bob. Consequently, Alice can choose to measure her particle (A) by the projective measurement in the general orthogonal basis $\{|0\rangle, |1\rangle\}$ and by a change of basis $\{|\Psi\rangle, |\Psi^{\perp}\rangle\}$ such that $\langle\Psi^{\perp}|\Psi\rangle = 0$. Hence, the shared maximally entangled state $|\Psi^{-}\rangle_{AB}$ in the general orthogonal basis is written as follows:

$$|\Psi^{-}\rangle_{\mathrm{AB}} = \frac{|\Psi\rangle_{\mathrm{A}}|\Psi^{\perp}\rangle_{\mathrm{B}} - |\Psi^{\perp}\rangle_{\mathrm{A}}|\Psi\rangle_{\mathrm{B}}}{\sqrt{2}} \tag{3.24}$$

Then, Alice applies the Von-Neumann measurement on the particle in her possession, which will give the result to either state $|\Psi\rangle$ or $|\Psi^{\perp}\rangle$ with a probability of one-half. Assuming the result of Alice projective measurement is the state $|\Psi^{\perp}\rangle$, the system will have the form:

$$|\Psi^{\perp}\rangle\langle\Psi^{\perp}|\Psi^{-}\rangle_{AB} = -\frac{|\Psi^{\perp}\rangle_{A} \otimes |\Psi\rangle_{B}}{\sqrt{2}} \tag{3.25}$$

After that, Alice sends her measurement result to Bob using one classical bit. Consequently, Bob will find the state of his particle in the target state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$. On the other hand, if the Alice projective measurement yielded state $|\Psi\rangle$, then by one classical bit, Alice informs Bob to apply a unitary transformation on his state to obtain its orthogonal complement. Note that, based on the entangled state, Alice and Bob share the proper Pauli operator Bob needs to apply on his state to obtain the target qubit. Therefore, the required resource to complete remote state preparation is one maximally entangled state as a quantum channel and one classical bit of information.

3.3 Physical Quantum Channels

In this model [54], Alice and Bob wish to establish a secret key for private communication, and a third party who is trusted will facilitate the quantum key distribution process operation. Our specific goal is to allow the parties to first agree on the bases. Once the agreement is made, the parties form a secret key using these bases. This protocol requires three quantum channels and two classical channels as shown in Figure 3.2.

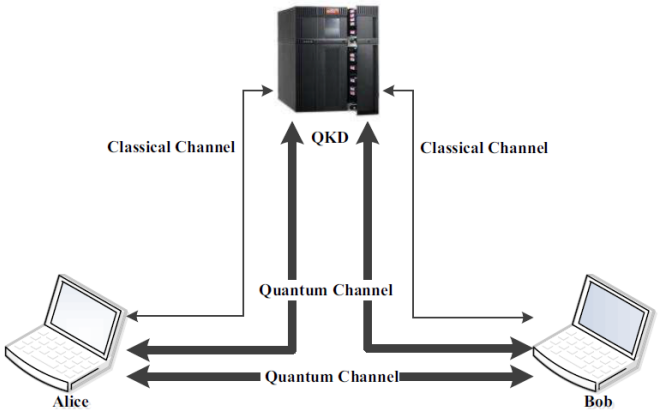

Figure 3.2 Three-Party Quantum Key Distribution

3.3.1 The Required Rounds

To determine the required rounds, we consider the probabilities of three aspects of this model. These aspects are related to the bases chosen randomly by each party and the QKD. Figure 3.3 shows all the possible probabilities in this protocol. Measuring a qubit in the correct basis results in a correct outcome. However, measuring a qubit in a wrong basis results in a random outcome with a probability of one-half that the outcome state is correct or incorrect.

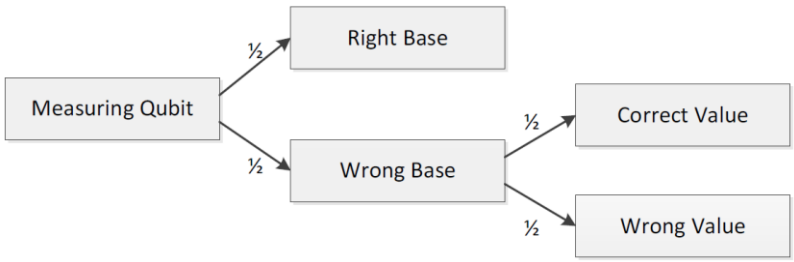

Figure 3.3 Probabilities in measuring qubits

To determine if a qubit is constant after several rounds of measurements, we calculate the following probabilities:

1. Both parties have the same basis and get correct outcomes in n rounds
2. The receiver measures a qubit using the wrong basis and gets the correct outcome
3. The receiver measures a qubit using the wrong basis and gets the wrong outcome

Calculating the probability that during n number of rounds the observed qubit will not change is as follows:

$$\mathrm{P} = \left(\frac{1}{2}\right)^{\mathrm{n}} * \left(\frac{1}{2}\right) * \left(\frac{1}{2}\right) = \left(\frac{1}{2}\right)^{\mathrm{n+2}} \tag{3.26}$$

From (3.26), we can calculate the probability of getting a correct outcome when the size of the secret key is m bits as follows:

$$\mathrm{C} = \left(\left(1 - \left(\frac{1}{2}\right)^{\mathrm{n}} * \left(\frac{1}{2}\right) * \left(\frac{1}{2}\right)\right)\right)^{\mathrm{m}} \tag{3.27}$$

$$\mathrm{C} = \left(1 - \left(\frac{1}{2}\right)^{\mathrm{n+2}}\right)^{\mathrm{m}} \tag{3.28}$$

We consider a target accuracy to achieve a specific accuracy for the secret key. The target accuracy determines the required rounds that the protocol must perform to gain enough information about the parties correct and incorrect bases. For example, let us set a target accuracy of 99%. Then, calculate the required rounds as shown in [55] as follows:

$$\left(1 - \left(\frac{1}{2}\right)^{\mathrm{n+2}}\right)^{\mathrm{m}} = 99\% \tag{3.29}$$

$$\sqrt[\mathrm{m}]{\left(1 - \left(\frac{1}{2}\right)^{\mathrm{n+2}}\right)^{\mathrm{m}}} = \sqrt[\mathrm{m}]{.99} \tag{3.30}$$

$$\left(1-\left(\frac{1}{2}\right)^{n+2}\right)^{m} = \sqrt[m]{.99} \tag{3.31}$$

$$-\left(\frac{1}{2}\right)^{n+2} = \sqrt[m]{.99} - 1 \tag{3.32}$$

$$\left(\frac{1}{2}\right)^{n+2} = 1 - \sqrt[m]{.99} \tag{3.33}$$

$$\log\left(\frac{1}{2}\right)^{n+2} = \log\left(1 - \sqrt[m]{.99}\right) \tag{3.34}$$

$$(n+2)\log\left(\frac{1}{2}\right) = \log\left(1 - \sqrt[m]{.99}\right) \tag{3.35}$$

$$\frac{(n+2)\log\left(\frac{1}{2}\right)}{\log\left(\frac{1}{2}\right)} = \frac{\log\left(1 - \sqrt[m]{.99}\right)}{\log\left(\frac{1}{2}\right)} \tag{3.36}$$

$$(n+2) = \log_2\left(1 - \sqrt[m]{.99}\right) \tag{3.37}$$

$$n = -\log_2\left(1 - (.99)^{\frac{1}{m}}\right) - 2 \tag{3.38}$$

From (3.38), we can determine the required number of rounds to achieve the target accuracy of 99%. So, n rounds are needed to achieve a specific secret key accuracy before requesting the parties to shift their bases.

3.3.2 Selecting the Key Size

Selecting the size of the secret key affects the number of rounds required to be performed to achieve the required accuracy of 99%. Let us assume that 500 bits is the size of the secret key. Then, the required rounds will be ≈ 14 as follows:

$$n = -\log_2\left(1 - (.99)^{\frac{1}{500}}\right) - 2 = 13.6 \tag{3.39}$$

As the key size increases, the number of rounds increases. However, the increase in the number of rounds is bounded as shown in Figure 3.4.

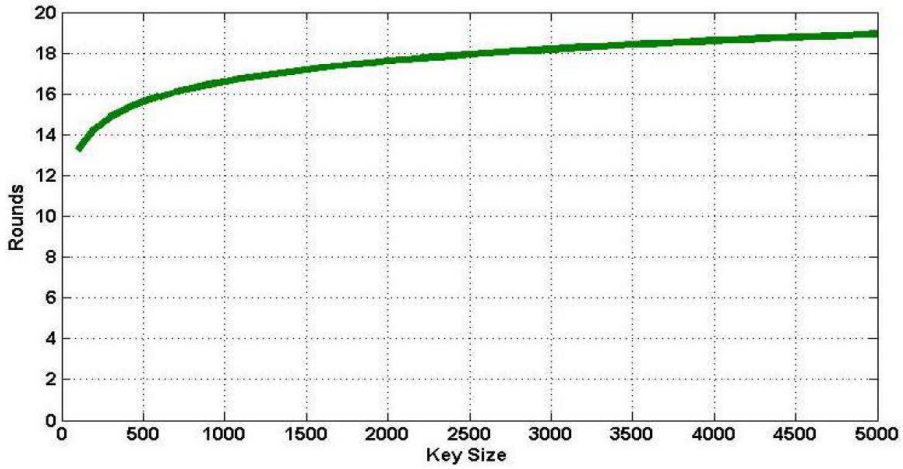

Figure 3.4 Relationship between key size and number of rounds

3.4 Entanglement-Assisted Quantum Channels

In this model [56], we assume that each party shares N EPR pairs with the trusted party named Charlie and does not share EPR pairs with the other parties. The first step in this model is to establish an EPR-pair between the sender and the receiver by the help of the trusted node Charlie Figure 3.5. After that, Charlie acts as a generator of the EPR-pairs between the sender and the receiver to allow them to communicate with each other.

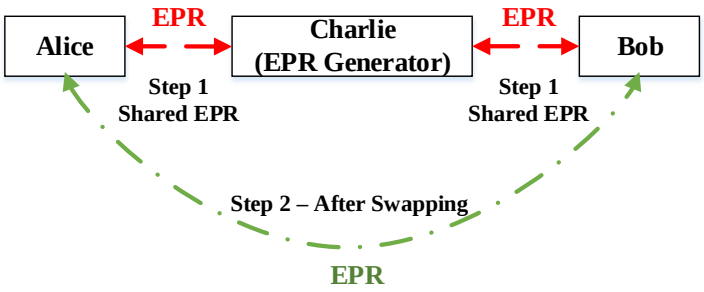

Figure 3.5 Establishing EPR pair by entanglement swapping

After forming the EPR pair between Alice and Bob, they have the option to measure their pair using one of the bases $|+\rangle, |-\rangle, |0\rangle \; or \; |1\rangle$. When Alice measures her state (first qubit in the EPR pair) using a basis, Bob's state (second qubit in the EPR pair) will be collapsed to the opposite of the result of Alice's state. However, for Bob to have the correct opposite state, he needs to measure his state using the same basis Alice used in her measurement.

$$|+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \tag{3.40}$$

$$|-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}} \tag{3.41}$$

$$|0\rangle = \frac{|+\rangle + |-\rangle}{\sqrt{2}} \tag{3.42}$$

$$|1\rangle = \frac{|+\rangle - |-\rangle}{\sqrt{2}} \tag{3.43}$$

Alice and Bob measure their qubit in one of the bases randomly. After that, they meet on the classical channel and compare their measurement basis of each state without disclosing their measurement result. If both use the same basis, their results are opposite to each other. For example, if Alice uses basis $|+\rangle, |-\rangle$ and her measurement results are state $|+\rangle$, the result of Bob's measurement will be $|-\rangle$. And if Alice uses basis $|0\rangle$, $|1\rangle$ for her measurement, if the result of her first qubit is $|1\rangle$, then the result of Bob's second qubit will be $|0\rangle$. At the end, Bob reverses all of his measurement results to have the same outcomes as Alice, which is the secret key.

3.5 Entanglement-Assisted Remote State Preparation Quantum Channels

This model [57] is based on two important algorithms in quantum computing. The first algorithm is entanglement swapping [58], and the second algorithm is the remote state preparation [11]. In this model, we establish EPR pairs between the sender Alice and the receiver Bob. Both Alice and Bob share EPR-pairs with an intermediate trusted node called Charlie, who will act as a generator of EPR pairs between Alice and Bob in the following states:

$$|\Psi^-\rangle_{AB} = \frac{1}{\sqrt{2}}(|0\rangle_A|1\rangle_B - |1\rangle_A|0\rangle_B) \tag{3.44}$$

$$|\Psi^+\rangle_{AB} = \frac{1}{\sqrt{2}}(|0\rangle_A|1\rangle_B + |1\rangle_A|0\rangle_B) \tag{3.45}$$

$$|\Phi^-\rangle_{AB} = \frac{1}{\sqrt{2}}(|0\rangle_A|0\rangle_B - |1\rangle_A|1\rangle_B) \tag{3.46}$$

$$|\Phi^+\rangle_{AB} = \frac{1}{\sqrt{2}}(|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B) \tag{3.47}$$

After establishing the EPR pairs, Alice remotely prepares a specific and known quantum state to share it with Bob. For example, if Alice wants to transmit a qubit in the pure state $|\Psi\rangle$ to Bob:

$$|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle \tag{3.48}$$

And, let us consider that their EPR pair is state $|\Psi^-\rangle_{AB}$. So, particle A belongs to Alice and particle B belongs to Bob. Now, Alice wants to transmit the known state $|\Psi\rangle$ to Bob. Alice

can choose to measure that state in any qubit basis, such as $|\Psi\rangle$, which is related to basis $|0\rangle_A$ as:

$$|0\rangle_A = \alpha|\Psi\rangle - \beta|\Psi\perp\rangle \tag{3.49}$$

Or measure that state in the qubit basis $|\Psi\perp\rangle$ which is related to basis $|1\rangle_A$ as:

$$|1\rangle_A = \beta^*|\Psi\rangle + \alpha|\Psi\perp\rangle \tag{3.50}$$

Writing the state $|\Psi^-\rangle_{AB}$ with these bases will result in:

$$|\Psi^-\rangle_{AB} = \frac{1}{\sqrt{2}}(|\Psi\rangle_A|\Psi\perp\rangle_B - |\Psi\perp\rangle_A|\Psi\rangle_B) \tag{3.51}$$

After Alice applies a Von Neumann measurement on a single particle, let us consider Alice's particle result to be in state $|\Psi\perp\rangle$. Then, the total state will be as follows:

$$|\Psi\perp\rangle_A\langle\Psi\perp|\Psi^-\rangle_{AB} = -\frac{1}{\sqrt{2}}|\Psi\perp\rangle_A \otimes |\Psi\rangle_B \tag{3.52}$$

When Alice sends the measurement result to Bob by sending only one classical bit, Bob will find the particle in state $\alpha|0\rangle_B + \beta|1\rangle_B$. However, when the measurement of Alice's particle is $|\Psi\rangle_A$, Bob will find it in the state:

$$|\Psi\perp\rangle = \beta^*|\Psi\rangle + \alpha|\Psi\perp\rangle \tag{3.53}$$

which is the complement to the original state. This method works on any EPR pair result from the entanglement swapping from the basis$\{|\Psi^{\pm}\rangle_{AB}, |\Phi^{\pm}\rangle_{AB}\}$. However, applying Pauli matrices $(\sigma_z, i\sigma_y, \sigma_x)$ will be needed to form the correct state based on the EPR pair used between Alice and Bob.

3.6 Mutually Authenticated Quantum Channels and Bell State Measurement

The previous protocols, in particular [59], do not offer mutual authentication and depend on the trusted authority to authenticate the users. Without mutual authentication, the communicating parties have no confidence that they are communicating with a trusted authority. Therefore, attacks such as replay, and man-in-the-middle are possible. In our model [60], we secure the registration process by mutual authentication. Also, the secret key is renewed after each use by distributing a new secret key after each successful authentication.

3.6.1 Mutual Authentication and Registration:

Consider a network of n users u_i, where i is the user identification number $u_i \in U = \{u_1, u_2, \dots, u_n\}$. Each user shares a secret key $k_{Tu}^{2m} \in K = \{k_{Tu}^1, k_{Tu}^2, \dots, k_{Tu}^{2m}\}$ of size $2m$, where $k_{Tu}^{2m} = \{k_{Tu1}^m + k_{Tu2}^m\}$ with the trusted user Trent. We assume that the key exchange occurred during the setup of each user in the network. If Alice wishes to communicate with Bob, she contacts Trent, who knows every user in the network. At the beginning, Trent and Alice need to build mutual authentication by identification and verification of each's identity. They use the shared secret key $k_{TA}^{2m} = \{k_{TA1}^m + k_{TA2}^m\}$ to derive the encoding bases $b_{TA}^{2m} = \{b_{TA1}^m + b_{TA2}^m\}$ from the bases $B_z = \{|0\rangle, |1\rangle\}$ and the bases $B_x = \{|+\rangle, |-\rangle\}$. For each bit in the secret key, they make the bits "0" and "1" correspond to bases B_z and B_x, respectively. After, Trent and Alice each generate a random sequence S_{TA} and S_{AT}, respectively, of size m and then encode it by the bases b_{TA1}^m.

Next, Trent and Alice exchange the encoded sequences. So, the legitimate Trent and Alice must be able to derive the decoding bases b_{TA1}^m from the secret key k_{TA1}^m and then decode each other's sequence. After, they meet on the classical channel. Trent announces Alice's S_{AT}^m and Alice announces Trent's sequence S_{TA}^m. Trent and Alice then verify their sequences; they continue if they receive the correct sequences so that they are mutually authenticated. If one of them receives the wrong sequence, they abandon the channel. After that, Trent contacts Bob and performs the same authentication process. Trent and Bob use the shared secret key $k_{TB}^{2m} = \{k_{TB1}^m + k_{TB2}^m\}$ to derive the encoding bases $b_{TA}^{2m} = \{b_{TB1}^m + b_{TB2}^m\}$. Next, Both Trent and Bob generate a random sequence S_{TB}^m and S_{BT}^m, respectively, of size m and then encode it by bases b_{TB1}^m. After, Trent and Bob exchange the encoded sequences and then meet on the classical channel to verify their sequences. Trent and Bob verify the sequences S_{TB}^m and S_{BT}^m, respectively, and then they continue if both receive the correct sequences or they abandon the channel. If no one has abandoned the channel, then Trent and Alice, as well as Trent and Bob, are mutually authenticated. Further, Trent will provide Alice and Bob with a secret key to create a secret sequence for authenticating before communication. Trent encodes the second part of Bob's secret key k_{TB2}^m by b_{TA2}^m and then sends it to Alice. Also, Trent encodes the second part of Alice's secret key k_{TA2}^m using b_{TB2}^m and then sends it to Bob.

3.6.2 Secret Key Distribution:

Trent builds the quantum channel after creating the mutual authentication between him and each of Alice and Bob. For each user, Trent prepares an *L* random Bell basis:

$$|\Upsilon(L)\rangle_{Tu} = \{|\Upsilon(1)\rangle_{Tu}, |\Upsilon(2)\rangle_{Tu}, \dots, |\Upsilon(\mathrm{L})\rangle_{Tu}\} \quad (3.54)$$

where $|\Upsilon\rangle \in \{|\Psi^-\rangle, |\Psi^+\rangle, |\Phi^-\rangle, |\Phi^+\rangle\}$, and then shares them with the user. Also, let i and j be the indexes of Alice and Bob states, respectively, where $i = j = t + q + p = L$. Trent shares the entangled pairs $|\Upsilon(i)\rangle_{TA}$ with Alice by keeping the first particle of $|\Upsilon(i)\rangle_T$ and sending the second particle $|\Upsilon(i)\rangle_A$ to Alice. Likewise, Trent shares the entangled pairs $|\Upsilon(j)\rangle_{TB}$ with Bob by keeping the first particles $|\Upsilon(j)\rangle_T$ and sending the second particle $|\Upsilon(j)\rangle_B$ to Bob. After, Alice randomly chooses $(t + q)/2$ inconsecutive states of her entanglement with Trent $|\Upsilon(L)\rangle_{TA}$ and then performs a Bell measurement on the state $|\Upsilon(i)\rangle_{TA} \otimes |\Upsilon(i + 1)\rangle_{TA}$. For example, if the random state i is $|\Phi^+(i)\rangle_{12}$, and the state $i + 1$ is $|\Phi^+(i + 1)\rangle_{34}$, where the particles 1 and 4 belong to Trent and the particles 2 and 3 belong to Alice. Then, Bell measurement on $|\Phi^+\rangle_{12} \otimes |\Phi^+\rangle_{34}$ will give one result of $\{|\Phi^+\rangle_{14}|\Phi^+\rangle_{23}\}$, $\{|\Phi^-\rangle_{14}|\Phi^-\rangle_{23}\}$, $\{|\Psi^+\rangle_{14}|\Psi^+\rangle_{23}\}$, or $|\Psi^-\rangle_{14}|\Psi^-\rangle_{23}$; each occurs with a probability of $1/4$. If Alice finds the state $|\Psi^+\rangle_{23}$, the state Trent holds should be $|\Psi^+\rangle_{14}$. For each measurement result, Alice represents the states $|\Phi\rangle$ and $|\Psi\rangle$ by the bits "0" and "1", respectively. In the same manner, she represents the phase of the states " $+$ " and " $-$ " by the bits "0" and "1" , respectively Figure 3.6. For error detection, Alice meets with Trent on the classical channel to inform him of the $t/2$ chosen pairs and the measurement result of each pair. Trent verifies if the results Alice obtained satisfy the Bell state measurement for the chosen $t/2$ pairs. If Trent finds the results do not satisfy Bell measurement, the channel is compromised, and they abandon the channel. However, if the results satisfy the Bell measurement for entanglement swapping, Trent and Alice represent the remaining $q/2$ pairs in bits and consider them an initial secret key r.

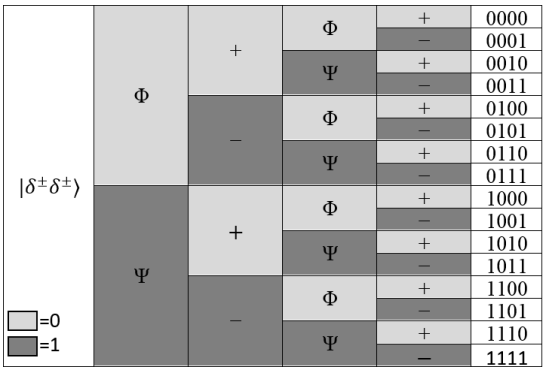

Figure 3.6 The representation of the states using classical bits.

3.6.3 Privacy Amplification

Consider a scenario where an attacker (Eve) listens to the classical channel and gains some information about the initial secret key. Then, another level of security is needed to reduce Eve's information. Therefore, Trent and Alice apply privacy amplification to derive a secret key with a low correlation to the initial key. We assume that every user shares with Trent a family of universal hash functions [61] GF with a uniform distribution of hash functions g, which maps n bits input A to m bits output B. Also, if $\{r_1, r_2\} \in A$ and g is randomly selected, $g(r_1) = g(r_2)$ with probability of $1/|B|$. Trent selects a hash function $g \in GF$ and then informs Alice through the classical channel which hash function was selected. Next, Trent and Alice feed the initial secret key into the hash function to obtain the final secret key $g(r) = k_{TA}^{m}$. Similarly, Trent follows the same process of verification and key distribution with Bob to obtain a new secret key k_{TB}^{m}.

3.6.4 Communication:

Trent reorders the p remaining entangled pairs between him and Alice:

$$|\Upsilon(i)\rangle_{TA} = \{|\Upsilon(1)\rangle_{TA}, |\Upsilon(2)\rangle_{TA}, \dots, |\Upsilon(p)\rangle_{TA}\} \quad (3.55)$$

and the remaining p entangled pairs between him and Bob:

$$|\Upsilon(j)\rangle_{TB} = \{|\Upsilon(1)\rangle_{TB}, |\Upsilon(2)\rangle_{TB}, \dots, |\Upsilon(p)\rangle_{TB}\} \quad (3.56)$$

Then, Trent performs entanglement swapping to create an entanglement state between Alice and Bob. Trent performs an entanglement swapping process using $|\Upsilon(i)\rangle_{TA} \otimes |\Upsilon(j)\rangle_{TB}$. Trent informs Alice and Bob about which state they share using two classical bits. Therefore, Alice and Bob will have their i and j states, respectively, entangled in one of the Bell states, each occurring with a probability of 1/4.

$$|\Psi^{-}(i,j)\rangle_{AB} = \frac{1}{\sqrt{2}}(|0\rangle_A|1\rangle_B - |1\rangle_A|0\rangle_B) \quad (3.57)$$

$$|\Psi^{+}(i,j)\rangle_{AB} = \frac{1}{\sqrt{2}}(|0\rangle_A|1\rangle_B + |1\rangle_A|0\rangle_B) \quad (3.58)$$

$$|\Phi^{-}(i,j)\rangle_{AB} = \frac{1}{\sqrt{2}}(|0\rangle_A|0\rangle_B - |1\rangle_A|1\rangle_B) \quad (3.59)$$

$$|\Phi^{+}(i,j)\rangle_{AB} = \frac{1}{\sqrt{2}}(|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B) \quad (3.60)$$

Alice and Bob use their entangled pairs to communicate using quantum communication protocols such as teleportation, Ekert 91, or remote state preparation. Alice and Bob make a final authentication to make sure that each party is the same party; Trent is authenticated in the first process. They use the secret key k_{TA2}^{m} and k_{TB2}^{m} , which Trent distributed to Bob and Alice, respectively. Each party derives the encoding basis and then creates and exchanges a secret sequence. Next, Alice and Bob meet on the classical channel to verify each other's sequence. The legitimate Alice and Bob should be able to decode and verify their identity. If one of them cannot decode the sequence and verify their identity, they

cannot trust each other and abandon the channel. However, if they are the legitimate Alice and Bob, they will be able to decode the sequences and have mutual authentication. So, Alice and Bob are authenticated to each other and are able to start the communication using the entanglement-assisted quantum communication protocols.

CHAPTER 4: DETERMINISTIC AND EFFICIENT THREE-PARTY QKD AND THE RESULTS

4.1 Introduction

In this chapter, an efficient and deterministic quantum key distribution protocol for establishing a secret key between two untrusted users is presented [7]. In this protocol, a secret key is distributed to a sender and a receiver who share entangled states with a third trusted party but not with each other. This secret key is distributed by means of special pure quantum states using remote state preparation and controlled gates. In addition, we employ the parity bits of the entangled pairs and ancillary states to assist in preparing and measuring the secret states. Distributing a state to two users requires two maximally entangled pairs as the quantum channel and a two-particle von Neumann projective measurement. The proposed protocol is exact and deterministic. It distributes a secret key of d qubits by means of $2d$ entangled pairs and, on average, d bits of classical communication. We demonstrate the security of this protocol against entanglement attacks and present a method of privacy amplification.

4.2 The Algorithm

Suppose that the sender Alice wishes to share a secret key with the receiver Bob. However, they do not have access to a physical quantum communication channel or share entangled pairs. Therefore, Alice contacts Charlie, who is a trusted party in a network of n

users, where $u_n \in U = \{u_1, u_2, \dots u_n\}$. With every user, he shares m maximally entangled pairs in the form $\{|\delta(1)\rangle_{12}, |\delta(2)\rangle_{12}, \dots, |\delta(m)\rangle_{12}\}$, where $|\delta(m)\rangle \in \{|\Psi^{\pm}\rangle, |\Phi^{\pm}\rangle\}$:

$$|\Psi^{\pm}\rangle_{12} = \frac{1}{\sqrt{2}}(|0\rangle_1|1\rangle_2 \pm |1\rangle_1|0\rangle_2) \tag{4.1}$$

$$|\Phi^{\pm}\rangle_{12} = \frac{1}{\sqrt{2}}(|0\rangle_1|0\rangle_2 \pm |1\rangle_1|1\rangle_2) \tag{4.2}$$

Particle 1 belongs to Charlie, and particle 2 belongs to the user. In addition, suppose that the qubit $|T\rangle_{Cu} = \{|0\rangle, |1\rangle\}$ represents the type of the entangled state, where the values '0' and '1' correspond to the states $|\Phi^{\pm}\rangle$ and $|\Psi^{\pm}\rangle$, respectively. In a maximally entangled state, taking the trace of particle 1 to find the reduced density operator of particle 2 results in a number multiplied by the identity operator I. For instance, the reduced density operator of particle 2 in the state $|\Phi^{+}\rangle_{12}$ is as follows:

$$\rho_2 = tr_1[|\Phi^{+}\rangle_{12\ 12}\langle\Phi^{+}|] = \frac{1}{2}\, I_2 \tag{4.3}$$

Therefore, measuring particle 1 in any basis results in a random state of $|0\rangle_1$ or $|1\rangle_1$, each occurring with a probability of $1/2$. Using their shared entangled states, Charlie distributes between Alice and Bob a random secret key of size p, where $k_p \in K = \{k_1, k_2, \dots k_p\}$. For each bit k_p, Charlie creates the corresponding pure state $|\Psi\rangle_p$ in the following form:

$$|\Psi\rangle_p = \cos\frac{\theta}{2}|0\rangle + \sin\frac{\theta^{i\phi}}{2}|1\rangle \tag{4.4}$$

Charlie chooses the coefficients $\cos(\theta/2)$ and $\sin(\theta/2)\exp(i\phi)$ to be real and complex numbers, respectively, where the angles θ and φ are real numbers such that $0 <$

$\theta < \pi$ and $0 < \varphi < 2\pi$. In addition, the coefficients satisfy the equation $|\cos(\theta/2)|^2 + |\sin(\theta/2)\exp(i\phi)|^2 = 1$. A state with the angle $\theta/2$ resides on the surface of the Bloch sphere, whereas a state with the angle $\theta = 0$ resides on the south or north pole of the Bloch sphere. Charlie measures the state $|\Psi\rangle_p$ by projecting it into the general qubit basis $\{|\Psi\rangle, |\Psi^{\perp}\rangle\}$, where $\langle\Psi^{\perp}|\Psi\rangle = 0$ and the basis states have the following form:

$$|\Psi\rangle = |0\rangle = \alpha|\Psi\rangle - \beta|\Psi^{\perp}\rangle \tag{4.5}$$

$$|\Psi^{\perp}\rangle = |1\rangle = \beta^{*}|\Psi\rangle + \alpha|\Psi^{\perp}\rangle \tag{4.6}$$

Let us suppose that Charlie projects the state $|\Psi\rangle_p$ into this basis and obtains the state $|\Psi\rangle$ given in (4.5). Also, suppose that the entangled state shared by Charlie and Alice is the state $|\Psi^{-}\rangle_{13}$ and that the entangled state shared by Charlie and Bob is the state $|\Psi^{-}\rangle_{24}$. Both pairs can be represented as follows:

$$|\Psi^{-}\rangle_{13} = \frac{1}{\sqrt{2}}(|0\rangle_1|1\rangle_3 - |1\rangle_1|0\rangle_3) \tag{4.7}$$

$$|\Psi^{-}\rangle_{24} = \frac{1}{\sqrt{2}}(|0\rangle_2|1\rangle_4 - |1\rangle_2|0\rangle_4) \tag{4.8}$$

where particles 1 and 2 belong to Charlie and particles 3 and 4 belong to Alice and Bob, respectively. The singlet state $|\Psi^{-}\rangle$ comprises two entangled anti-correlated particles with a total spin of zero. The nature of this state is such that if we measure the first particle and find it to be in a given direction, then the second particle must be in the opposite direction. For example, if we measure the first particle by means of a projection along the Z axis, $Z\otimes I$, and find it to be in the state $|1\rangle_1$, then the second particle must be in the state $|0\rangle_1$. Moreover, the singlet state can be written in the general qubit basis $\{|\Psi\rangle, |\Psi^{\perp}\rangle\}$ as follows:

$$|\Psi^-\rangle_{13} = \frac{1}{\sqrt{2}}(|\Psi\rangle_1|\Psi^\perp\rangle_3 - |\Psi^\perp\rangle_1|\Psi\rangle_3) \tag{4.9}$$

$$|\Psi^-\rangle_{24} = \frac{1}{\sqrt{2}}(|\Psi\rangle_2|\Psi^\perp\rangle_4 - |\Psi^\perp\rangle_2|\Psi\rangle_4) \tag{4.10}$$

Charlie can view his shared states with Alice and Bob as follows:

$$|\Psi^-\rangle_{13} \otimes |\Psi^-\rangle_{24} = \frac{1}{\sqrt{2}}[(|0\rangle_1|1\rangle_3 - |1\rangle_1|0\rangle_3) \otimes (|0\rangle_2|1\rangle_4 - |1\rangle_2|0\rangle_4)] \tag{4.11}$$

Through a change of basis, the states become as follows:

$$\begin{aligned} |\Psi^-\rangle_{13} \otimes |\Psi^-\rangle_{24} = \frac{1}{\sqrt{2}}[&(|\Psi\rangle_1|\Psi^\perp\rangle_3 - |\Psi^\perp\rangle_1|\Psi\rangle_3) \\ &\otimes (|\Psi\rangle_2|\Psi^\perp\rangle_4 - |\Psi^\perp\rangle_2|\Psi\rangle_4)] \end{aligned} \tag{4.12}$$

Charlie can view the entire quantum channel shared with Alice and Bob as follows:

$$\begin{aligned} |\Upsilon\rangle_{1234} = \frac{1}{2}[&|\Psi\rangle_1|\Psi\rangle_2|\Psi^\perp\rangle_3|\Psi^\perp\rangle_4 - |\Psi\rangle_1|\Psi^\perp\rangle_2|\Psi^\perp\rangle_3|\Psi\rangle_4 \\ &-|\Psi^\perp\rangle_1|\Psi\rangle_2|\Psi\rangle_3|\Psi^\perp\rangle_4 + |\Psi^\perp\rangle_1|\Psi^\perp\rangle_2|\Psi\rangle_3|\Psi\rangle_4] \end{aligned} \tag{4.13}$$

Now, Charlie measures his particles by performing a two-particle projection measurement in the orthogonal qubit basis $\{|\Psi\rangle, |\Psi^\perp\rangle\}$:

$$P_{1\{\Psi,\Psi^\perp\}} \otimes P_{2\{\Psi,\Psi^\perp\}} \otimes I \otimes I|\Upsilon\rangle_{1234} \tag{4.14}$$

where the operators P_Ψ and $P_{\Psi^\perp}$ are:

$$P_\Psi = |\Psi\rangle\langle\Psi| \tag{4.15}$$

$$P_{\Psi^\perp} = |\Psi^\perp\rangle\langle\Psi^\perp| \tag{4.16}$$

The measurement results in a certain state with a probability of 1/4. After the measurement, each particle is in either the state $|\Psi\rangle_{\{1,2\}} = \alpha|\Psi\rangle_{\{1,2\}} - \beta^*|\Psi^\perp\rangle_{\{1,2\}}$ or the state $|\Psi^\perp\rangle_{\{1,2\}} =$

$\beta^*|\Psi\rangle_{\{1,2\}} + \alpha|\Psi^\perp\rangle_{\{1,2\}}$, each with a probability of $1/2$. All possible measurement outcomes are summarized in Table 4.1.

Table 4.1 All possible states after the two-particle projective measurement performed by Charlie and the collapse of the entangled states of Alice and Bob.

Probability	Measurement	State
$1/4$	$\|\Psi\rangle_1, \|\Psi\rangle_2$	$\|\Psi\rangle_1\|\Psi\rangle_2\|\Psi^\perp\rangle_3\|\Psi^\perp\rangle_4$
$1/4$	$\|\Psi\rangle_1, \|\Psi^\perp\rangle_2$	$-\|\Psi\rangle_1\|\Psi^\perp\rangle_2\|\Psi^\perp\rangle_3\|\Psi\rangle_4$
$1/4$	$\|\Psi^\perp\rangle_1, \|\Psi\rangle_2$	$-\|\Psi^\perp\rangle_1\|\Psi\rangle_2\|\Psi\rangle_3\|\Psi^\perp\rangle_4$
$1/4$	$\|\Psi^\perp\rangle_1\|\Psi^\perp\rangle_2$	$\|\Psi^\perp\rangle_1\|\Psi^\perp\rangle_2\|\Psi\rangle_3\|\Psi\rangle_4$

Suppose that Charlie's measurement result is $\{|\Psi\rangle_1, |\Psi^\perp\rangle_2\}$; then, the total state $|\Upsilon\rangle_{1234}$ becomes as follows:

$$\begin{aligned} &\langle\Psi|\Psi\rangle_1 \otimes \langle\Psi^\perp|\Psi^\perp\rangle_2 \otimes I \otimes I|\Upsilon\rangle_{1234} \\ &= -\frac{1}{2}[\langle\Psi|\Psi\rangle_1 \otimes \langle\Psi^\perp|\Psi^\perp\rangle_2 \otimes |\Psi^\perp\rangle_3 \otimes |\Psi\rangle_4] \end{aligned} \tag{4.17}$$

Consequently, the state Alice holds collapses to:

$$|\Psi\rangle_1\langle\Psi|\Psi^-\rangle_{13} = -\frac{1}{2}[|\Psi\rangle_1 \otimes |\Psi^\perp\rangle_3] \tag{4.18}$$

and the state Bob holds collapses to:

$$|\Psi^\perp\rangle_2\langle\Psi^\perp|\Psi^-\rangle_{24} = -\frac{1}{2}[|\Psi^\perp\rangle_2 \otimes |\Psi\rangle_4] \tag{4.19}$$

Let us suppose that Charlie has a prior agreement with the parties to create an ancillary qubit in the state $|0\rangle$ which, later becomes the control bit a unitary operator. Therefore, Alice and Bob each prepare an ancillary qubit $|0\rangle_{\{A,B\}}$ for each entangled pair

they share with Charlie. So, their states become $|\Psi^{-}\rangle_{13}|0\rangle_{A}$ and $|\Psi^{-}\rangle_{24}|0\rangle_{B}$ for Alice and Bob respectively. To distribute the secret state $|\Psi\rangle_{p}$ to each party, Charlie performs two controlled-NOT gates ($CNOT_{C1}, CNOT_{C2}$), and each user performs a controlled-NOT gate ($CNOT_{u1}$) and a controlled-U gate from the set $\{Ucx_{u1}, Ucy_{u1}\}$. The controlled-U gates are defined as follows:

$$Ucx = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}, Ucy = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & -i \\ 0 & 0 & i & 0 \end{bmatrix} \tag{4.20}$$

The inputs to $CNOT_{C1}$ are the states $|\Psi\rangle_{p}$ and $|\Psi\rangle_{1}$. The state $|\Psi\rangle_{p} = 0$ is the control, and the state $|\Psi\rangle_{1} = 0$ is the target; therefore, $|0_{p}, 0_{1}\rangle \rightarrow |0_{p}, 0_{1} \oplus 0_{p}\rangle$, which results in the state $|0_{p}, 0_{1}\rangle$. The inputs to $CNOT_{C2}$ are the states $|\Psi\rangle_{1}$ and $|T\rangle_{CA}$, where the state $|\Psi\rangle_{1} = 0$ from the previous gate is the control and the state $|T\rangle_{CA} = 1$ is the target. Thus, the gate becomes $|0_{1}, 1_{CA}\rangle \rightarrow |0_{1}, 1_{CA} \oplus 0_{1}\rangle$, which results in the state $|0_{1}, 1_{CA}\rangle$. The state of $|T\rangle_{CA}$ indicates to Charlie the state to which the state Alice holds has collapsed after the projective measurement. Finding $|T\rangle_{CA} = 1$ indicates that Alice holds an incorrect state, which needs to be corrected through a unitary transformation. Therefore, Charlie sends to Alice one classical bit $|T\rangle_{CA} = 1$. Alice inputs the received bit and the ancillary state $|0\rangle_{A}$ into $CNOT_{A1}$, where $|T\rangle_{CA} = 1$ is the control state and the ancillary state $|0\rangle_{A} = 0$ is the target; therefore, $|1_{CA}, 0_{A}\rangle \rightarrow |1_{CA}, 0_{A} \oplus 1_{CA}\rangle$, which results in $|1_{CA}, 1_{A}\rangle$. Subsequently, Alice inputs the new ancillary state $|1\rangle_{A}$ and her state $|\Psi^{\perp}\rangle_{3}$ from equation (4.18) into Ucy_{A}, where the new ancillary state $|1\rangle_{A} = 1$ is the control and the state $|\Psi^{\perp}\rangle_{3}$ is the target, i.e., $Ucy_{A}(|1\rangle_{A} \otimes |\Psi^{\perp}\rangle_{3})$, which results in $|1_{A}, \Psi_{3}\rangle$. Thus, Alice transforms her state into its orthogonal complement $|\Psi\rangle_{3} = 0$, which is the same as the state that

Charlie wanted to send, $|\Psi\rangle_p = 0$. Table 4.2 summarizes all possible outcomes and the actions required from Charlie and Alice for the different measurement results. The quantum circuit between Charlie and Alice is depicted in Figure 4.1.

Table 4.2 All possible outcomes of different inputs and the actions required from Charlie and Alice.

Charlie	Ancillary	Alice
$\|0_p, 0_1, 0_{CA}\rangle$	$\|0\rangle_A$	$Ucy_A\|0\rangle_A\|\Psi\rangle_3$
$\|0_p, 0_1, 1_{CA}\rangle$	$\|1\rangle_A$	$Ucy_A\|1_A\rangle\|\Psi^{\perp}\rangle_3$
$\|0_p, 1_1, 0_{CA}\rangle$	$\|1\rangle_A$	$Ucy_A\|1_A\rangle\|\Psi^{\perp}\rangle_3$
$\|0_p, 1_1, 1_{CA}\rangle$	$\|0\rangle_A$	$Ucy_A\|0\rangle_A\|\Psi\rangle_3$
$\|1_p, 0_1, 0_{CA}\rangle$	$\|1\rangle_A$	$Ucy_A\|1_A\rangle\|\Psi\rangle_3$
$\|1_p, 0_1, 1_{CA}\rangle$	$\|0\rangle_A$	$Ucy_A\|0\rangle_A\|\Psi^{\perp}\rangle_3$
$\|1_p, 1_1, 0_{CA}\rangle$	$\|0\rangle_A$	$Ucy_A\|0\rangle_A\|\Psi^{\perp}\rangle_3$
$\|1_p, 1_1, 1_{CA}\rangle$	$\|1\rangle_A$	$Ucy_A\|1_A\rangle\|\Psi\rangle_3$

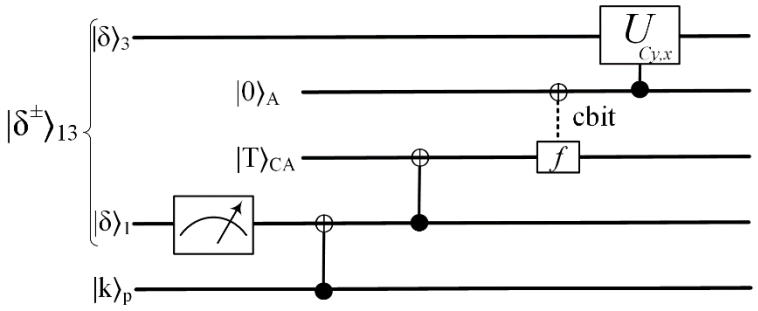

Figure 4.1 Shows the quantum circuit between Charlie and Alice.

Charlie performs the same distribution process with Bob. From (4.19), Charlie obtains the state $|\Psi^{\perp}\rangle_2$ from his shared entangled state with Bob. The secret key state $|\Psi\rangle_p = 0$ and the state obtained by Charlie, $|\Psi^{\perp}\rangle_2 = 1$, are the inputs to $CNOT_{C1}$; therefore, $|0_p, 1_2\rangle \rightarrow |0_p, 1_2 \oplus 0_p\rangle$ results in $|0_p, 1_2\rangle$. In addition, the states $|\Psi^{\perp}\rangle_2 = 1$

and $|T\rangle_{CB} = 1$ are the inputs to $CNOT_{C2}$, so $|1_2, 1_{CB}\rangle \rightarrow |1_2, 1_{CB} \oplus 1_2\rangle$ results in $|1_2, 0_{CB}\rangle$. Finding $|T\rangle_{CB} = 0$ tells Charlie that Bob has the correct state, so Charlie sends no information to Bob, and the ancillary state $|0\rangle_B$ remains unchanged. Therefore, Bob applies Ucy_B using the ancillary state $|0\rangle_B = 0$ as the control and the state $|\Psi\rangle_4 = 0$ as the target, i.e., $Ucy_B[|0\rangle_B \otimes |\Psi\rangle_4]$, which results in $|0_A, \Psi_4\rangle$. The state that Bob holds remains unchanged because it is the same as the secret key state $|\Psi\rangle_p = 0$ that Charlie wanted to send. Figure 4.2 shows the complete quantum circuit between Charlie, Alice, and Bob.

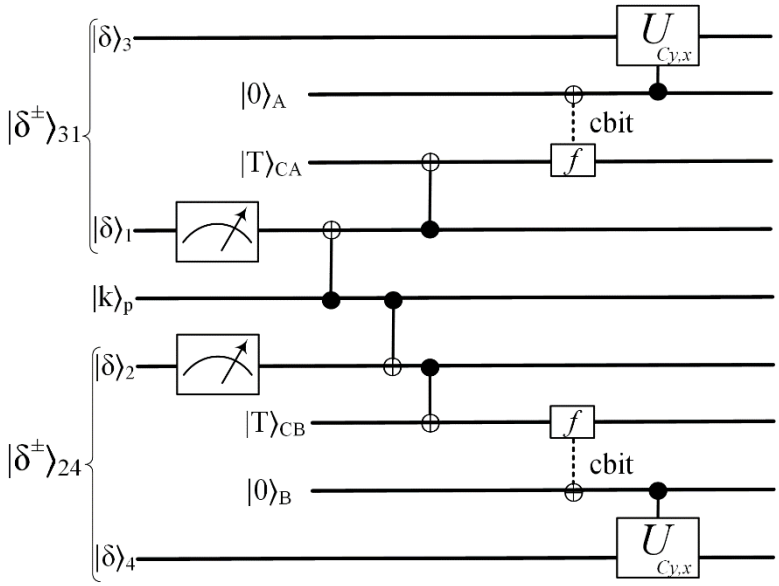

Figure 4.2 Quantum circuit between Charlie, Alice, and Bob.

If the two-particle projective measurement described by (4.13) results in the states $\{|\Psi\rangle_1, |\Psi\rangle_2\}$, then the overall state $|\Upsilon\rangle_{1234}$ becomes as follows:

$$\langle\Psi|\Psi\rangle_1 \otimes \langle\Psi|\Psi\rangle_2 \otimes I \otimes I|\Upsilon\rangle_{1234} = \frac{1}{2}[\langle\Psi|\Psi\rangle_1 \otimes \langle\Psi|\Psi\rangle_2 \otimes |\Psi^{\perp}\rangle_3 \otimes |\Psi^{\perp}\rangle_4] \quad (4.21)$$

Charlie finds the state $|T\rangle_{CA} = 1$ and the state $|T\rangle_{CB} = 1$ for the entangled states shared with Alice and Bob, respectively. Therefore, to distribute the state $|\Psi\rangle_p$ to Alice and Bob, Charlie sends one classical bit, $|T\rangle_{CA} = |T\rangle_{CB} = 1$, to each of them through the classical channel. If the two-particle projective measurement described by (4.13) yields the states $\{|\Psi^{\perp}\rangle_1, |\Psi\rangle_2\}$, then the overall state $|\Upsilon\rangle_{1234}$ becomes as follows:

$$\begin{aligned} &\langle\Psi^{\perp}|\Psi^{\perp}\rangle_1 \otimes \langle\Psi|\Psi\rangle_2 \otimes I \otimes I|\Upsilon\rangle_{1234} \\ &= \frac{1}{2}\langle\Psi^{\perp}|\Psi^{\perp}\rangle_1 \otimes \langle\Psi|\Psi\rangle_2 \otimes |\Psi\rangle_3 \otimes |\Psi^{\perp}\rangle_4] \end{aligned} \tag{4.22}$$

Thus, $|T\rangle_{CA} = 0$ and $|T\rangle_{CB} = 1$. Therefore, Alice's ancillary state remains unchanged, and Charlie sends one classical bit, $|T\rangle_{CB} = 1$, to Bob. Finally, if the two-particle projective measurement described by (4.13) yields the states $\{|\Psi^{\perp}\rangle_1, |\Psi^{\perp}\rangle_2\}$, then the overall state $|\Upsilon\rangle_{1234}$ will be as follows:

$$\begin{aligned} &\langle\Psi^{\perp}|\Psi^{\perp}\rangle_1 \otimes \langle\Psi^{\perp}|\Psi^{\perp}\rangle_2 \otimes I \otimes I|\Upsilon\rangle_{1234} \\ &= \frac{1}{2}\langle\Psi^{\perp}|\Psi^{\perp}\rangle_1 \otimes \langle\Psi^{\perp}|\Psi^{\perp}\rangle_2 \otimes |\Psi^{\perp}\rangle_3 \otimes |\Psi\rangle_4] \end{aligned} \tag{4.23}$$

Consequently, Charlie will find the state $|T\rangle_{CA} = 0$ and the state $|T\rangle_{CB} = 0$. Alice and Bob will successfully obtain the state that Charlie wanted to distribute by using the ancillary states $|0\rangle_A$ and $|0\rangle_B$ to control their target states. Table 4.3 summarizes the process of distributing a state between Alice and Bob when they share $|\Psi^{-}\rangle_{13} \otimes |\Psi^{-}\rangle_{24}$.

At this point, Alice's and Bob's qubits correspond to the same state, which they call k_p. Charlie repeats the same process for the next bit, k_{p+1}. After p such processes by Charlie, Alice and Bob will share the secret key $K = \{k_1, k_2, \ldots k_p\}$. This protocol is exact

Table 4.3 Summary of the process of distributing a state between Alice and Bob.

Probability	Charlie	$\|T\rangle_{CA}$	$\|T\rangle_{CB}$	cbit	Alice	Bob
$1/4$	$\|\Psi\rangle_1, \|\Psi\rangle_2$	1	1	2	$Ucy_A\|1\rangle_A\|\Psi^{\perp}\rangle_3$	$Ucy_B\|1\rangle_B\|\Psi^{\perp}\rangle_4$
$1/4$	$\|\Psi\rangle_1, \|\Psi^{\perp}\rangle_2$	1	-	1	$Ucy_A\|1\rangle_A\|\Psi^{\perp}\rangle_3$	$Ucy_B\|0\rangle_B\|\Psi\rangle_4$
$1/4$	$\|\Psi^{\perp}\rangle_1, \|\Psi\rangle_2$	-	1	1	$Ucy_A\|0\rangle_A\|\Psi\rangle_3$	$Ucy_B\|1\rangle_B\|\Psi^{\perp}\rangle_4$
$1/4$	$\|\Psi^{\perp}\rangle_1, \|\Psi^{\perp}\rangle_2$	-	-	-	$Ucy_A\|0\rangle_A\|\Psi\rangle_3$	$Ucy_B\|0\rangle_B\|\Psi\rangle_4$

and deterministic. Moreover, it is based on RSP for the distribution of a chosen state on the equator or the polar great circle of the Bloch sphere. According to (4.17), (4.21), (4.22) and (4.23) the average cost of distributing such a secret key between Alice and Bob is one classical bit of information. Therefore, the cost of sending d qubits is $2d$ entangled pairs and d classical bits on average. The transformation of an arbitrary pure state into its orthogonal complement is known to be anti-unitary and thus cannot be achieved. However, a rotation around some axis of an equatorial or polar state is equivalent to the anti-unitary transformation that transforms a state into its orthogonal complement. Therefore, through prior agreement with both parties, Charlie prepares their states on the pole, $|\psi\rangle = \cos\theta|0\rangle + \sin\theta^{i\phi}|1\rangle$, or on the equator, $|\psi\rangle = (|0\rangle + e^{i\phi}|1\rangle)/\sqrt{2}$, of the Bloch sphere. If Charlie prepares a state in the polar form, then either party can obtain its orthogonal complement by performing the unitary transformation Ucy, which performs a $\pi -$ rotation around the y-axis of that state Figure 4.3. If they instead agree to prepare their states in the equatorial form, then either party can obtain the orthogonal complement by performing the unitary transformation Ucx, which performs a $\pi -$ rotation around the x-axis of that state.

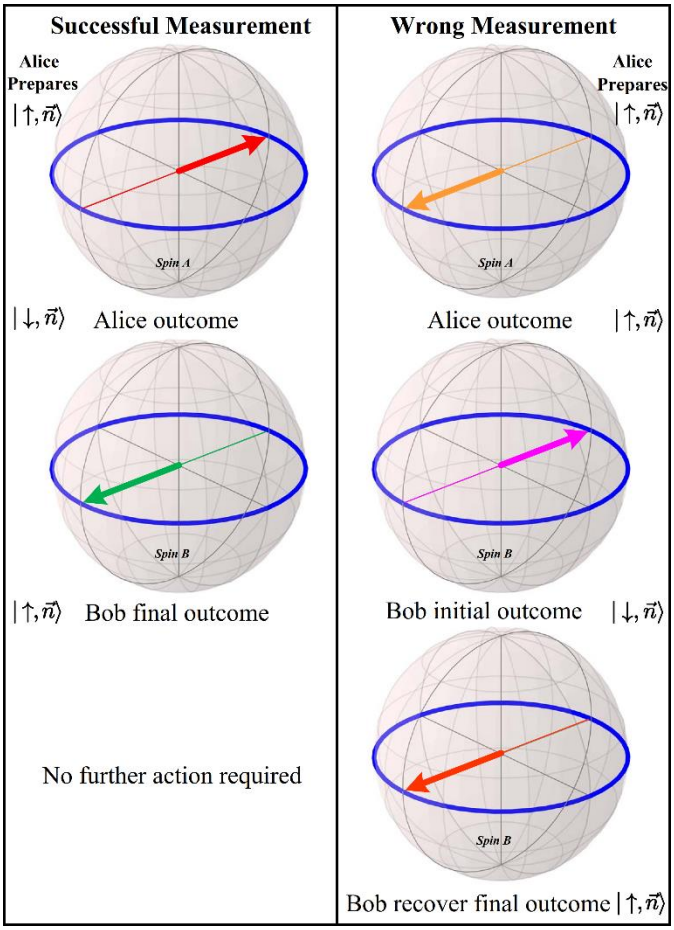

Figure 4.3 Show remote state preparation operation. In the successful measurement, Alice prepares a state which in Bloch sphere is demonstrate as an arrow. In the successful measurement, Alice measurement of her *A* spin yields the complement of the prepared state and Bob yield the correct state. In the wrong measurement, Alice measurement results in the prepared state so Bob get the opposite of that state. Therefore, Bob need to perform a rotation to recover the state Alice intended to send.

Furthermore, Charlie can share any maximally entangled pair $\{|\Phi^{\pm}\rangle, |\Psi^{\pm}\rangle\}$ with Alice and Bob. For example, let us suppose that Charlie and Alice share the state $|\Phi^{+}\rangle_{13}$ and that Charlie and Bob share the state $|\Psi^{+}\rangle_{24}$:

$$|\Phi^+\rangle_{13} \otimes |\Psi^+\rangle_{24} = \frac{1}{\sqrt{2}}[(|0\rangle_1|0\rangle_3 + |1\rangle_1|1\rangle_3) \otimes (|0\rangle_2|1\rangle_4 + |1\rangle_2|0\rangle_4)] \quad (4.24)$$

Through a change of basis, the entangled states can be written as follows:

$$|\Phi^+\rangle_{13} \otimes |\Psi^+\rangle_{24} = \frac{1}{\sqrt{2}}[\left(|\Psi\rangle_1(i\sigma_y)|\Psi^\perp\rangle_3 + |\Psi^\perp\rangle_1(i\sigma_y)|\Psi\rangle_3\right) \otimes (|\Psi\rangle_2(i\sigma_z)|\Psi^\perp\rangle_4 + |\Psi^\perp\rangle_2(i\sigma_z)|\Psi\rangle_4)] \quad (4.25)$$

Performing a two-particle projection measurement on the total state $|\Upsilon\rangle_{1234}$ results in a certain state with a probability of 1/4. Table 4.4 summarizes all possible outcomes of the two-particle measurement when the quantum channel consists of $|\Phi^+\rangle_{13}$ and $|\Psi^+\rangle_{24}$.

Table 4.4 All possible outcomes of the two-particle projection measurement.

Probability	Measurement	State
$1/4$	$\|\Psi\rangle_1, \|\Psi\rangle_2$	$\|\Psi\rangle_1, \|\Psi\rangle_2, (i\sigma_y)\|\Psi^\perp\rangle_3, (\sigma_z)\|\Psi^\perp\rangle_4$
$1/4$	$\|\Psi\rangle_1, \|\Psi^\perp\rangle_2$	$-\|\Psi\rangle_1, \|\Psi^\perp\rangle_2, (i\sigma_y)\|\Psi^\perp\rangle_3, (\sigma_z)\|\Psi\rangle_4$
$1/4$	$\|\Psi^\perp\rangle_1, \|\Psi\rangle_2$	$-\|\Psi^\perp\rangle_1, \|\Psi\rangle_2, (i\sigma_y)\|\Psi\rangle_3, (\sigma_z)\|\Psi^\perp\rangle_4$
$1/4$	$\|\Psi^\perp\rangle_1, \|\Psi^\perp\rangle_2$	$\|\Psi^\perp\rangle_1, \|\Psi^\perp\rangle_2, (i\sigma_y)\|\Psi\rangle_3, (\sigma_z)\|\Psi\rangle_4$

Let us assume that Charlie obtained the states $|\Psi^\perp\rangle_1$ and $|\Psi^\perp\rangle_2$ and that the secret key state is $|\Psi\rangle_p = 0$. In addition, the qubits $|T\rangle_{CA} = |\Phi^+\rangle_{13} = 0$ and $|T\rangle_{CB} = |\Psi^+\rangle_{24} = 1$ indicate the types of the entangled states that Charlie shares with Alice and Bob, respectively. Therefore, based on the types of the entangled pairs, the states held by Alice and Bob must collapse to $|\Psi^\perp\rangle_3$ and $|\Psi\rangle_4$, respectively. After applying the controlled gates, Alice and Bob obtain the secret state $|\Psi\rangle_p$ by applying $Ucy_A(|1\rangle_A \otimes (i\sigma_y|\Psi^\perp\rangle_3))$ and $Ucy_B(|0\rangle_B \otimes (\sigma_z|\Psi\rangle_4))$, respectively. Furthermore, when Charlie and Alice share the

state $|\Psi^-\rangle_{13}$ and Charlie and Bob share one of $\{|\Psi^\pm\rangle, |\Phi^\pm\rangle\}$, then all possible quantum channels can be written as follows:

$$|\Psi^-\rangle_{13} \otimes |\Psi^-\rangle_{24} = \frac{1}{\sqrt{2}}[(|\Psi\rangle_1(\sigma_0)|\Psi^\perp\rangle_3 - |\Psi^\perp\rangle_1(\sigma_0)|\Psi\rangle_3) \otimes (|\Psi\rangle_2(\sigma_0)|\Psi^\perp\rangle_4 - |\Psi^\perp\rangle_2(\sigma_0)|\Psi\rangle_4)] \tag{4.26}$$

$$|\Psi^-\rangle_{13} \otimes |\Psi^+\rangle_{24} = \frac{1}{\sqrt{2}}[(|\Psi\rangle_1(\sigma_0)|\Psi^\perp\rangle_3 - |\Psi^\perp\rangle_1(\sigma_0)|\Psi\rangle_3) \otimes -(|\Psi\rangle_2(\sigma_z)|\Psi^\perp\rangle_4 + |\Psi^\perp\rangle_2(\sigma_z)|\Psi\rangle_4)] \tag{4.27}$$

$$|\Psi^-\rangle_{13} \otimes |\Phi^+\rangle_{24} = \frac{1}{\sqrt{2}}[(|\Psi\rangle_1(\sigma_0)|\Psi^\perp\rangle_3 - |\Psi^\perp\rangle_1(\sigma_0)|\Psi\rangle_3) \otimes \left(|\Psi\rangle_2(i\sigma_y)|\Psi^\perp\rangle_4 + |\Psi^\perp\rangle_2(i\sigma_y)|\Psi\rangle_4\right)] \tag{4.28}$$

$$|\Psi^-\rangle_{13} \otimes |\Phi^-\rangle_{24} = \frac{1}{\sqrt{2}}[(|\Psi\rangle_1(\sigma_0)|\Psi^\perp\rangle_3 - |\Psi^\perp\rangle_1(\sigma_0)|\Psi\rangle_3) \otimes (|\Psi\rangle_2(\sigma_x)|\Psi^\perp\rangle_4 - |\Psi^\perp\rangle_2(\sigma_x)|\Psi\rangle_4)] \tag{4.29}$$

When Charlie and Alice share $|\Psi^+\rangle_{13}$ and Charlie and Bob share one of $\{|\Psi^\pm\rangle, |\Phi^\pm\rangle\}$, then all possible quantum channels can be written as follows:

$$|\Psi^+\rangle_{13} \otimes |\Psi^+\rangle_{24} = \frac{1}{\sqrt{2}}[-(|\Psi\rangle_1(\sigma_z)|\Psi^\perp\rangle_3 + |\Psi^\perp\rangle_1(\sigma_z)|\Psi\rangle_3) \otimes -(|\Psi\rangle_2(\sigma_z)|\Psi^\perp\rangle_4 + |\Psi^\perp\rangle_2(\sigma_z)|\Psi\rangle_4)] \tag{4.30}$$

$$|\Psi^+\rangle_{13} \otimes |\Psi^-\rangle_{24} = \frac{1}{\sqrt{2}}[-(|\Psi\rangle_1(\sigma_z)|\Psi^\perp\rangle_3 + |\Psi^\perp\rangle_1(\sigma_z)|\Psi\rangle_3) \otimes (|\Psi\rangle_2(\sigma_0)|\Psi^\perp\rangle_4 - |\Psi^\perp\rangle_2(\sigma_0)|\Psi\rangle_4)] \tag{4.31}$$

$$|\Psi^+\rangle_{13} \otimes |\Phi^+\rangle_{24} = \frac{1}{\sqrt{2}}[-(|\Psi\rangle_1(\sigma_z)|\Psi^\perp\rangle_3 + |\Psi^\perp\rangle_1(\sigma_z)|\Psi\rangle_3) \tag{4.32}$$

$$\otimes \left(|\Psi\rangle_2(i\sigma_y)|\Psi^{\perp}\rangle_4 + |\Psi^{\perp}\rangle_2(i\sigma_y)|\Psi\rangle_4\right)]$$

$$|\Psi^{+}\rangle_{13} \otimes |\Phi^{-}\rangle_{24} = \frac{1}{\sqrt{2}}[-(|\Psi\rangle_1(\sigma_z)|\Psi^{\perp}\rangle_3 + |\Psi^{\perp}\rangle_1(\sigma_z)|\Psi\rangle_3) \otimes (|\Psi\rangle_2(\sigma_x)|\Psi^{\perp}\rangle_4 - |\Psi^{\perp}\rangle_2(\sigma_x)|\Psi\rangle_4)] \quad (4.33)$$

When Charlie and Alice share $|\Phi^{+}\rangle_{13}$ and Charlie and Bob share one of $\{|\Psi^{\pm}\rangle, |\Phi^{\pm}\rangle\}$, then all possible quantum channels can be written as follows:

$$|\Phi^{+}\rangle_{13} \otimes |\Psi^{+}\rangle_{24} = \frac{1}{\sqrt{2}}[\left(|\Psi\rangle_1\left(i\sigma_y\right)|\Psi^{\perp}\rangle_3 + |\Psi^{\perp}\rangle_1\left(i\sigma_y\right)|\Psi\rangle_3\right) \otimes (-|\Psi\rangle_2(\sigma_z)|\Psi^{\perp}\rangle_4 + |\Psi^{\perp}\rangle_2(\sigma_z)|\Psi\rangle_4)] \quad (4.34)$$

$$|\Phi^{+}\rangle_{13} \otimes |\Psi^{-}\rangle_{24} = \frac{1}{\sqrt{2}}[\left(|\Psi\rangle_1\left(i\sigma_y\right)|\Psi^{\perp}\rangle_3 + |\Psi^{\perp}\rangle_1\left(i\sigma_y\right)|\Psi\rangle_3\right) \otimes (|\Psi\rangle_2(\sigma_0)|\Psi^{\perp}\rangle_4 - |\Psi^{\perp}\rangle_2(\sigma_0)|\Psi\rangle_4)] \quad (4.35)$$

$$|\Phi^{+}\rangle_{13} \otimes |\Phi^{+}\rangle_{24} = \frac{1}{\sqrt{2}}[\left(|\Psi\rangle_1\left(i\sigma_y\right)|\Psi^{\perp}\rangle_3 + |\Psi^{\perp}\rangle_1\left(i\sigma_y\right)|\Psi\rangle_3\right) \otimes \left(|\Psi\rangle_2(i\sigma_y)|\Psi^{\perp}\rangle_4 + |\Psi^{\perp}\rangle_2(i\sigma_y)|\Psi\rangle_4\right)] \quad (4.36)$$

$$|\Phi^{+}\rangle_{13} \otimes |\Phi^{-}\rangle_{24} = \frac{1}{\sqrt{2}}[\left(|\Psi\rangle_1\left(i\sigma_y\right)|\Psi^{\perp}\rangle_3 + |\Psi^{\perp}\rangle_1\left(i\sigma_y\right)|\Psi\rangle_3\right) \otimes (|\Psi\rangle_2(\sigma_x)|\Psi^{\perp}\rangle_4 - |\Psi^{\perp}\rangle_2(\sigma_x)|\Psi\rangle_4)] \quad (4.37)$$

When Charlie and Alice share $|\Phi^{-}\rangle_{13}$ and Charlie and Bob share one of $\{|\Psi^{\pm}\rangle, |\Phi^{\pm}\rangle\}$, then all possible quantum channels can be written as follows:

$$|\Phi^{-}\rangle_{13} \otimes |\Psi^{+}\rangle_{24} = \frac{1}{\sqrt{2}}[(|\Psi\rangle_1(\sigma_x)|\Psi^{\perp}\rangle_3 - |\Psi^{\perp}\rangle_1(\sigma_x)|\Psi\rangle_3) \otimes (-|\Psi\rangle_2(\sigma_z)|\Psi^{\perp}\rangle_4 + |\Psi^{\perp}\rangle_2(\sigma_z)|\Psi\rangle_4)] \quad (4.38)$$

$$|\Phi^-\rangle_{13} \otimes |\Psi^-\rangle_{24} = \frac{1}{\sqrt{2}}[(|\Psi\rangle_1(\sigma_x)|\Psi^\perp\rangle_3 - |\Psi^\perp\rangle_1(\sigma_x)|\Psi\rangle_3) \otimes (|\Psi\rangle_2(\sigma_0)|\Psi^\perp\rangle_4 - |\Psi^\perp\rangle_2(\sigma_0)|\Psi\rangle_4)] \tag{4.39}$$

$$|\Phi^-\rangle_{13} \otimes |\Phi^+\rangle_{24} = \frac{1}{\sqrt{2}}[(|\Psi\rangle_1(\sigma_x)|\Psi^\perp\rangle_3 - |\Psi^\perp\rangle_1(\sigma_x)|\Psi\rangle_3) \otimes (|\Psi\rangle_2(i\sigma_y)|\Psi^\perp\rangle_4 + |\Psi^\perp\rangle_2(i\sigma_y)|\Psi\rangle_4)] \tag{4.40}$$

$$|\Phi^-\rangle_{13} \otimes |\Phi^-\rangle_{24} = \frac{1}{\sqrt{2}}[(|\Psi\rangle_1(\sigma_x)|\Psi^\perp\rangle_3 - |\Psi^\perp\rangle_1(\sigma_x)|\Psi\rangle_3) \otimes (|\Psi\rangle_2(\sigma_x)|\Psi^\perp\rangle_4 - |\Psi^\perp\rangle_2(\sigma_x)|\Psi\rangle_4)] \tag{4.41}$$

4.3 Modeling The Protocol

We model the protocol in this section. The model can be divided to three major components. Specifically, the source, the channel and the detector. In this model, we consider a PDC source located in the middle between Charlie and each one of Alice and Bob as shown in Figure 4.4. For instance, the type-II PDC source in Figure 4.4-A generates and distributes two entangled pairs in modes a_1 and b_1 to Alice and Bob respectively. Where, $i \in \{H, V\}$ represents the rectilinear polarization. Figure 4.5 shows the schematic diagram of the protocol between all the parties.

4.3.1 Source

The Hamiltonian of a type-II PDC with rotating-wave approximation (RWA) is given in [62] as:

$$H = i\kappa(a_H^\dagger b_V^\dagger - a_V^\dagger b_H^\dagger) + H.c. \tag{4.42}$$

Where κ is the result of multiplying the coupling value and the pump amplitude between the nonlinear crystal and the electromagnetic field. Also, $H.c.$ is the Hermition conjugate. Also, $a_i^\dagger b_i^\dagger$ and a_i, b_i are the annihilation and the creation operators respectively.

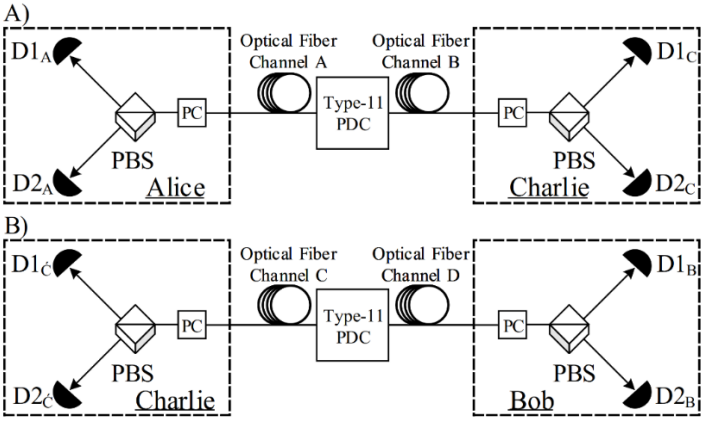

Figure 4.4 A schematic representation of the PSC process. The EPR source is located in the middle between two parties. A) Between Alice and Charlie. B) Between Charlie and Bob.

Therefore, as in [62] and [63] a type-II PDC source can create the following state:

$$|\Psi\rangle = \frac{1}{(\cosh\chi)^{-1}} \sum_{m=0}^{n} \sqrt{n+1}\tanh^n\chi \tag{4.43}$$

where $|\Phi_n\rangle$ is:

$$|\Phi_n\rangle = \frac{1}{\sqrt{n+1}} \sum_{m=0}^{n} (-1)_{ab}^{m} \tag{4.44}$$

which is a state of n-photon pairs of horizontal and vertical components. Therefore, following (4.43) the of the process of PDF to generate n-photon pairs is given by:

$$P(n) = \frac{(n+1)\lambda^n}{(1+\lambda)^{n+2}} \tag{4.45}$$

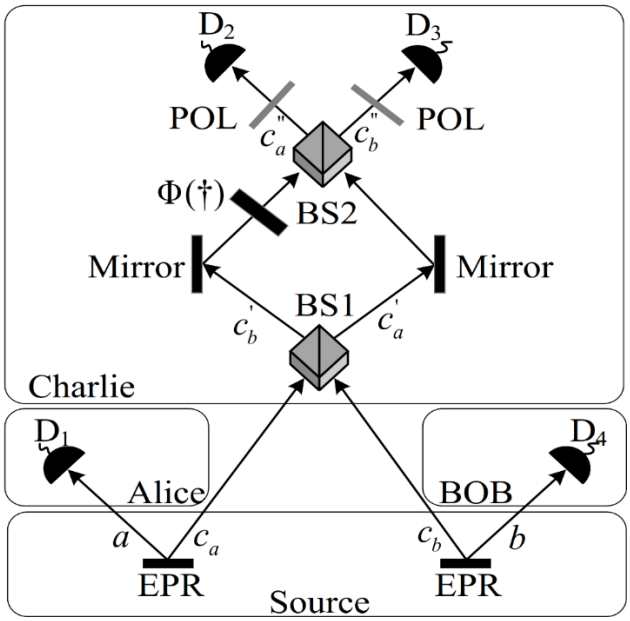

Figure 4.5 Shows the entanglement source and the three-parties. The distributed pairs pass through the interferometer. The pairs pass through the first beam splitter $BS1$ and the phase modulator Φ(†). Then, they pass through the second beam splitter $BS2$ and the polarizers POL to the detectors.

4.3.2 Channel

We consider the state generated by the EPR source between Alice and Charlie is the single state $|\Psi^-\rangle_{ac_a}$:

$$|\Psi^-\rangle_{ac_a} = \frac{1}{\sqrt{2}}[|H\rangle_a|V\rangle_{c_a} - |V\rangle_a|H\rangle_{c_a}] \equiv \frac{1}{\sqrt{2}}(a_H^\dagger b_V^\dagger - a_V^\dagger b_H^\dagger)|0\rangle_a|0\rangle_{c_a} \qquad (4.46)$$

and the state generated by the EPR source between Charlie and Bob is the single state $|\Psi^-\rangle_{cb_b}$:

$$|\Psi^-\rangle_{cb_b} = \frac{1}{\sqrt{2}}[|H\rangle_{c_b}|V\rangle_b - |V\rangle_{c_b}|H\rangle_b] \equiv \frac{1}{\sqrt{2}}(a_H^\dagger b_V^\dagger - a_V^\dagger b_H^\dagger)|0\rangle_{c_b}|0\rangle_b \qquad (4.47)$$

Therefore, the entire system state in the channel becomes:

$$\frac{1}{2}(a_H^\dagger b_V^\dagger - a_V^\dagger b_H^\dagger)(c_H^\dagger d_V^\dagger - c_V^\dagger d_H^\dagger)|0\rangle_a|b\rangle_{c_a}|0\rangle_{c_b}|0\rangle_b \quad (4.48)$$

$$= a_H^\dagger d_V^\dagger b_V^\dagger c_H^\dagger - a_H^\dagger d_H^\dagger b_V^\dagger c_V^\dagger - a_V^\dagger d_V^\dagger b_H^\dagger c_H^\dagger + a_V^\dagger d_H^\dagger b_H^\dagger c_V^\dagger \quad (4.49)$$

4.3.3 Detector

Following [64] if we choose the phase $\Phi(t) = 0$ so $\Theta = 0$ then a detector receives:

$$= a_H^\dagger b_V^\dagger c_{aV}''^\dagger c_{bH}''^\dagger - a_H^\dagger b_H^\dagger c_{aV}''^\dagger c_{bV}''^\dagger - a_V^\dagger b_V^\dagger c_{aH}''^\dagger c_{bH}''^\dagger + a_V^\dagger b_H^\dagger c_{aH}''^\dagger c_{bV}''^\dagger \quad (4.50)$$

However, if we choose the phase $\Phi\ (t) = \frac{\pi}{2}$ then the detector receives:

$$= a_H^\dagger b_V^\dagger[-c_{aV}''^\dagger c_{bH}''^\dagger + c_{bV}''^\dagger c_{aH}''^\dagger] + a_V^\dagger b_H^\dagger[-c_{aH}''^\dagger c_{bV}''^\dagger + c_{bH}''^\dagger c_{aV}''^\dagger] \quad (4.51)$$

4.4 Security Analysis and Discussion

Charlie shares with each party maximally entangled pure states that contain two qubits, as described in equations (4.1) and (4.2). Taking the trace of particle 1 to find the reduced density operator of particle 2 results in a number multiplied by the identity operator $\rho_2 = (1/2)(I_2)$, as shown in equation (4.3). This implies that in any basis, the measurement Charlie performs results in an absolutely random state. Therefore, Charlie obtains either the state $|\Psi\rangle$ or the state $|\Psi^\perp\rangle$, each with a probability of $1/2$. Performing a local measurement on the particle that belongs to Charlie or the user reveals no information about the method used to prepare the state. However, a random bit will be generated after such a measurement. Therefore, Charlie projects the secret key state $|\Psi\rangle_p$ into his part of the entangled state ρ_1 to obtain an outcome from the set of v possible outcomes {0,1}, all of which occur with the same probability p. Charlie sends one classical bit T to the relevant party, indicating the unitary transformation U_T that the user should apply. Hence, sending

the type of unitary transformation to the party reveals no information about any particle. The party reconstructs the target state as $\rho_2 = (p_v)U_v|\Psi\rangle U_v^\dagger$. Thus, Charlie helps the party to prepare the target state. An attacker cannot obtain the secret key without knowledge of the entanglement type and the outcomes of the measurement.

Let us consider the entanglement attack, which is also called the EPR attack. Suppose that during entanglement distribution, Eve prepares $2m$ entangled pairs in the form $|\Psi^m\rangle_{ij} = |0\rangle_i|1\rangle_j - |1\rangle_i|0\rangle_j$. In addition, Eve intercepts every particle Charlie sends to Alice from the state $|\Psi^-\rangle_{13} = |0\rangle_1|1\rangle_3 - |1\rangle_1|0\rangle_3$ and forwards particle j instead. Therefore, Eve shares the state $|\Psi^-\rangle_{13}$ with Charlie and shares the state $|\Psi^-\rangle_{ij}$ with Alice. In addition, Eve can view the total state $|\Psi^-\rangle_{13} \otimes |\Psi^-\rangle_{ij}$ after the change of basis as follows:

$$\begin{aligned} &= \frac{1}{2}[|\Psi\rangle_1|\Psi\rangle_i|\Psi^\perp\rangle_3|\Psi^\perp\rangle_j - |\Psi\rangle_1|\Psi^\perp\rangle_i|\Psi^\perp\rangle_3|\Psi\rangle_j \\ &-|\Psi^\perp\rangle_1|\Psi\rangle_i|\Psi\rangle_3|\Psi^\perp\rangle_j + |\Psi^\perp\rangle_1|\Psi^\perp\rangle_i|\Psi\rangle_3|\Psi\rangle_j] \end{aligned} \tag{4.52}$$

Any measurement will collapse the total state to a result with a probability of 1/4. Therefore, the states of Charlie and Alice will correspond to each other with a probability of 1/2. Also, Alice prepares the correct states with a probability of 1/2 and the protocol fails because Eve cannot manipulate the classical information sent from Charlie. However, an attacker might gain some information about the key if the channel is noisy. For example, in a channel with ϵ noise, the upper bound of information Eve can gain about K is given by:

$$P = \frac{1}{2}(1+\epsilon)^p \tag{4.53}$$

So, for a noiseless channel $\epsilon = 0$ Eve can predict a given bit with probability of $P = 1/2$. Let us assume that Eve gained some information about the secret key. Therefore, Alice and Bob need to increase the security of the key by privacy amplification.

Therefore, for a noiseless channel ($\epsilon = 0$), Eve can predict a given bit with a probability of $P = 1/2$. Let us assume that Eve has gained some information about the secret key. Therefore, Alice and Bob need to increase the security of their key through privacy amplification. We assume that they share a family of universal hash functions [61] GF with a uniform hash function distribution g, where each hash function maps an n-bit input A to an m-bit output C. If $\{r_1, r_2\} \in A$ and g is randomly selected, then $g(r_1) = g(r_2)$ with a probability of $1/|C|$. To select a hash function, Alice and Bob divide K into j blocks B of h bits and then calculate the parity bit p for each block. Each block becomes $B_j + p_j \in K' = \{B_1 + p_1, B_2 + p_2, \dots B_j + p_j\}$, and the parity bits of the blocks are $P = \{p_1, p_2, \dots p_j\}$. Alice and Bob use P as an index to select the hash function $g \in GF$. Afterward, Alice and Bob feed K' into the hash function to obtain the final secret key $g(K') = K''$.

4.5 Results

Let us compare our protocol with other protocols in the literature Table 2.1. In this comparison, we consider the resources consumed to distribute a qubit from the trusted party to the sender and the receiver. Specifically, we compare the protocols based on the amount of entanglement and the classical bit consumption required to distribute a quantum state to the sender and the receiver Table 4.5.

Table 4.5 RSP algorithms dealing with three parties

Article	Q	E	C	Ch. Entanglement	State Type	Parties	S	R	Deter/Prob	Success	L.O.	S.M	R.M
[32]	6	2	3	Maximally GHZ	Special	3	2	1	Probabilistic	1/4	Pauli	Projective	Unitary
[37]	1	1	2	Maximally Tripartite	Special	3	1	2	Deterministic	1	σ_z	Projective	Unitary
[39]	1	2	2	Maximally Tripartite	Special	3	1	2	Deterministic	1	σ_z	Projective	Unitary
[42]	1	1	2	Maximally	Mixed	3	2	1	Probabilistic	1/2	σ_z	Projective	Unitary
[40]	1	1	3	Maximally GHZ	Special	3	1	2	Deterministic	1	σ_z	Projective	Unitary
[41]	2	5	2.5	Non-Maximally	Mixed	3	1	2	Probabilistic	1/2	Pauli	Projective	Unitary
[33]	3	3	<3.8	Maximally GHZ	Mixed	3	2	1	Probabilistic	1/2	Pauli	Projective	Unitary
[33]	3	3	4	Non-Maximally	Mixed	3	2	1	Probabilistic	1/8	Pauli	Projective	Unitary
[44]	1	1	2	Non-Maximally GHZ	Special	3	2	1	Probabilistic	1/2	σ_x	Projective	Projective
[45]	2	3	1	Maximally GHZ	Special	3	2	1	Probabilistic	1/2	Pauli	Projective	Unitary
[46]	2	2	3	Maximally GHZ	Special	3	1	2	Deterministic	1	Pauli	Projective	Unitary
[47]	1	2	2	Dark State	Special	3	1	2	Deterministic	1	$i\sigma_z$	Projective	Unitary
[48]	3	2	6	Maximally GHZ 4-P	W	3	2	1	Deterministic	1	CNOT	Projective	Unitary
[32]	2	1	4	Cluster State 6-P	Mixed	3	2	1	Probabilistic	1/4	$\sigma_z \otimes \sigma_z$	Projective	Unitary
[33]	2	2	<6.4	Maximally GHZ	Mixed	3	2	1	Deterministic	1	Pauli	Projective	Unitary
[43]	2	2	6	Non-Maximally GHZ	Special	3	1	2	Probabilistic	1/2	Pauli	Projective	Unitary
[35]	2	2	4	Maximally GHZ	Special	3	2	1	Probabilistic	1/2	Pauli	Projective	Unitary
[36]	5	4	7	Maximally GHZ 4-P	Brown State	3	2	1	Deterministic	1	Pauli	Projective	Unitary

In addition, we compare the protocols using the intrinsic efficiency equation presented in [65].

$$\eta = \frac{q_s}{q_u + b_t} \tag{4.54}$$

where q_s is the number of distributed qubits, q_u is the number of entangled bits in the quantum channel, and b_t is the number of classical communication bits. Table 4.6 summarizes the comparison between our protocol and similar protocols in the literature.

Table 4.6 Comparison of our protocol with related protocols in the literature.

No.	Protocol	Operations	Qubit/Type	Ebit/Type	Cbit	η
1	Ref [39]	2-Proj M[1], 2-U. Op[2]	2-Eq[3]	6-Triparatite	2	$1/4$
2	Ref [37]	1-Proj M, 2-U. Op	2-Eq	6-Triparatite	2	$1/4$
3	Ref [40]	2-Proj M, 3-U. Op	2-Eq	6-GHZ	2	$1/4$
4	Ref [46]	1-Proj M,1-BSM[4], 3-U. Op	2-Eq	6-GHZ	3	$2/9$
5	Ours	1-Proj M, 2-U. Op	2-Eq	4-EPR	1	$2/5$

[1] Projective measurement. [2] Unitary Operator, [3] Equatorial, [4] Bell state measurement

The protocol proposed in [39] distributes an equatorial state to two parties using a quantum channel consisting of two tripartite states and two bits of classical information. Therefore, it has an intrinsic efficiency of 1/4. The protocol presented in also has an efficiency of 1/4. It also distributes a qubit using two tripartite states as the quantum channel and two classical bits. In [46] a scheme for distributing a general qubit state to two users is proposed that uses two entangled states as the quantum channel and three bits of classical communication. Therefore, the efficiency of this protocol is 2/9. Finally, the scheme presented in [40] for distributing a quantum state to two parties uses two entangled Greenberger-Horne-Zeilinger (GHZ) states as the quantum channel and 2 classical bits. Therefore, it has an efficiency of 1/4. In our protocol, we distribute a quantum state to two users using a quantum channel consisting of two entangled states and one bit of classical communication on average, resulting in an efficiency of 2/5 Figure 4.6.

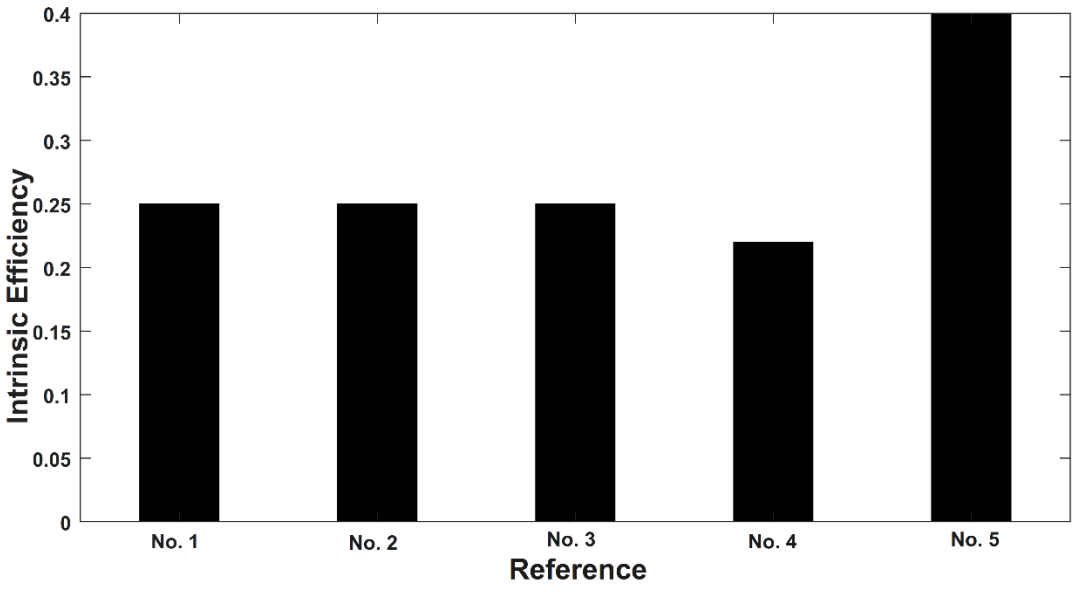

Figure 4.6 Shows comparison of the protocols based on the intrinsic efficiency.

CHAPTER 5: ENTANGLEMENT DISTRIBUTION IN MON AND THE RESULTS

5.1 Introduction

In this chapter, we present our quantum entanglement distribution architecture [8]. The main challenges are finding a dynamic distribution mechanism and reducing the physical impairments. Therefore, we start by presenting the backbone network and the design of the dynamic backbone nodes. Then, we define the wavelengths of the classical and the quantum communication channels. Next, we study the physical impairments in the defined channels. Specifically, we study Raman scattering, which is the main physical impairment when the launch power of the shorter wavelength classical signal is greater than the launch power of the longer wavelength quantum signal. We show the impact of Raman Stokes-shift on the signals of the quantum channel. After that, we show a simple design of entanglement distribution in an access network. Finally, we present the complete architecture and the numerical results for the entire network.

5.2 Backbone Network

In our design, the backbone network connects many access networks and has a ring topology. Reconfigurable optical add/drop multiplexers (ROADM) are nodes in the backbone for selective wavelength adding, dropping, or passing. Optical line terminals (OLT) are nodes at the end of point-to-point links to multiplex a set of wavelengths into a single fiber and demultiplex a set of wavelengths into multiple fibers. We are considering

CWDM as the multiplexing technique in the core network, which is a typical technique in the telecommunication infrastructures. Based on the ITU standards, the CWDM grid has 18 channels between 1270 nm and 1610 nm for spacing of 20 nm. We place a ROADM on the backbone for each access network and OLT between the ROADM and the access network component. The OLT does not require a transponder because all the signals will have a wavelength that matches CWDM or DWDM. ROADM handles traffic between the backbone and the access network by adding, dropping, or passing specific signals Figure 5.1. We designed the ROADM using an eight-channel CWDM multiplexer and a 32x32 Micro-electro-mechanical systems (MEMS) optical switch Figure 5.2. The insertion losses of the multiplexer and the optical switch are 1.5 and 1 dBm, respectively, as shown in Table 1 [66]. When the backbone traffic arrives at the ROADM, it gets demultiplexed in the backbone/ROADM to eight channels and passes to the optical switch inputs 1 to 8. If a signal does not belong to the current access network, the switch passes it to the corresponding 1 to 8 output to be multiplexed in the backbone/ROADM, and then it passes to the backbone. A signal belonging to the access network passes to outputs 9 to 16 for multiplexing in the AN/ROADM and then passes to the access network. Access network outbound traffic gets demultiplexed in the AN/ROADM. Then, it passes to the switch in inputs 9 to 16. It gets multiplexed in the backbone/ROADM and then sent to the backbone. This node introduces an insertion loss of 4 dBm for passing, dropping, or adding traffic.

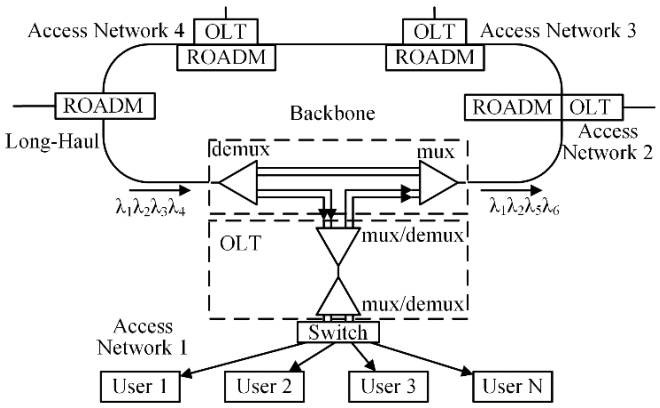

Figure 5.1 This MON has four access networks. Incoming traffic from the backbone arrives at the ROADM for dropping in the access network, adding data from the access network to the backbone, or directly passing to the backbone.

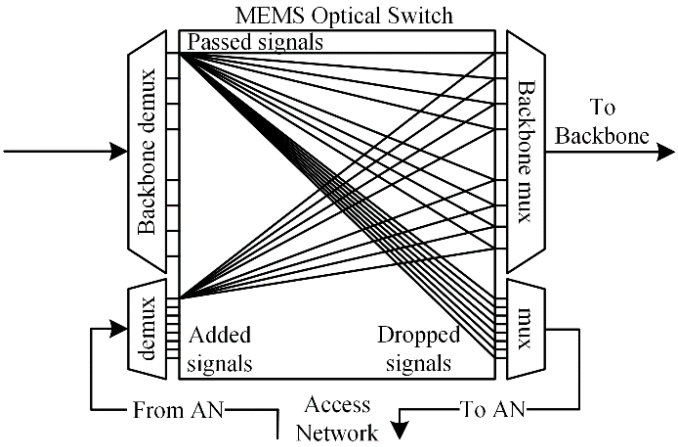

Figure 5.2. ROADM is made of a multiplexer/demultiplexer and MEMS optical switch. The optical switch is reconfigurable remotely to route the inputs from the demultiplexer to either the backbone for passing or the access network mux for dropping. The access network demultiplexer passes signals to the switch, which are then routed to the backbone.

5.3 Assignment of Quantum and Classical Channels

Applications of quantum cryptography require two communication channels: a quantum channel to send physical quantum states and a classical channel for information

reconciliation and privacy amplification. So, transmitting quantum and classical signals in the same network is important. However, in fiber-optic communication, the launch power of the classical signals is much stronger than the launch power of the quantum signals. So, nonlinear interaction occurs from Raman scattering and four-wave mixing (FWM). For this reason, the overlap between classical and quantum signals becomes difficult to reject. Therefore, we separate the quantum and the classical signals to travel in different spectral bands. The classical signals travel in the original O-band (1260-1360). Also, the quantum signals travel within the S-band (1460-1530), C-band (1530-1565), and L-band (1565-1625). In addition, the quantum signals travel in the low loss region as the typical attenuation loss in 1300 nm is 0.4 dBm/km, while in 1550 nm, it is 0.25 dBm/km. Based on the ITU grid standards for the CWDM, the space between channels is 20 nm. Moreover, a pair of entangled states can travel in the S-band at 1531-1571 nm and at 1511-1591 nm [67]. Consequently, entangled states can be created in DWDM or CWDM ITU channels by fine adjustment of the light source power in the SPDC process.

5.4 Physical Impairments

The infrastructures of optical networks can transmit a classical signal even with the existence of crosstalk. Given this, the added noise is 40 dBm less than the launch power of the original signal. The launch power of classical channels can be 100 dBm greater than the launch power of the quantum signals. Therefore, classical and quantum channels react differently to the physical impairments that occur within the channels. The source of noise in the optical networks mainly arises from FWM and Raman scattering. Additionally, amplified spontaneous emission generated from optical amplifiers and weak isolation from

the classical channels affect the quantum signals [68]. The Interaction in fiber optics that occurs between two or more pumps and fiber optic X^3 nonlinearity causes the FWM. FWM produces most of the noise in short distance links when the frequencies are close to each other. However, in practice, separated frequencies and long distance links make the effect of the FWM much weaker than the effect of Raman scattering. To show that the impact of FWM is not within our defined channels, we set a two continuous wave pump to 0 dBm and then vary the separation between the wavelengths Figure 5.3. As a result, the impact of FWM decreases and becomes very weak when the channel spacing is equal to or larger than 20nm. Additionally, polarization multiplexing and improving channel configuration reduces the impact of the FWM [69]. Thus, we will examine the effects that Raman scattering has on the quantum channels.

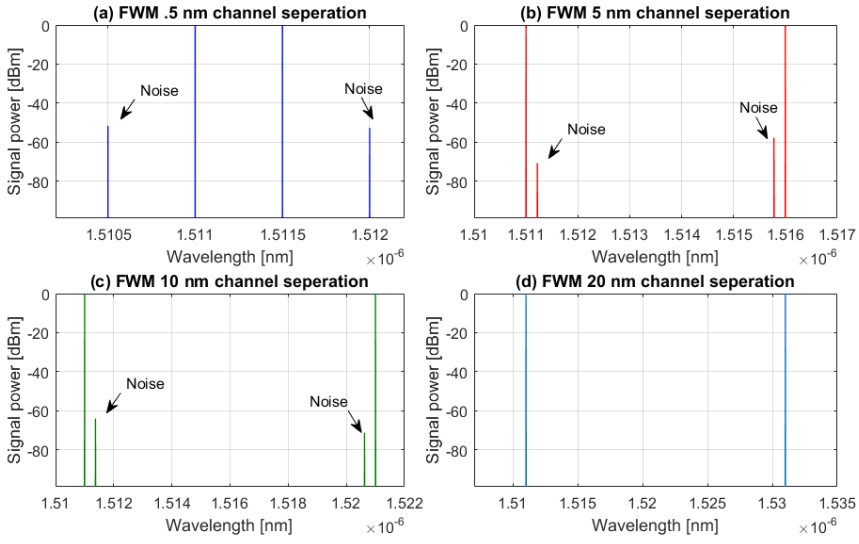

Figure 5.3. Shows the FWM with respect to different separations between two continuous wave (cw) pumps with launch power of 0 dBm. Increasing the channel separation and the distance decreases the FWM effect.

5.5 Raman Scattering

In stimulated Raman scattering (SRS), the power of the lower-wavelength channels transfers to the higher-wavelength channels. The interactions between the photons change their wavelength. Subsequently, this affects other channels in the medium. Increasing or decreasing a photon energy results in generating photons with higher and lower wavelengths than the original photons, which are referred to as Stokes and anti-Stokes, respectively. Stimulated Brillouin scattering (SBS), which is based on the vibrational energy, has a lower effect on the quantum channel because it has a frequency shift of 10 GHz. The SBS shift is small, especially for CWDM networks with a spacing grid of 20 nm. However, Raman scattering has a larger frequency shift up to 15 THz with an intensity peak at 13 THz. The direction of the frequency shift caused by the flat dispersion is free from the scattering direction. Therefore, a frequency shift occurs in the directions of the propagation as well as the direction of counter propagation [70]. The Raman frequency shift is given by:

$$hv' = hv \pm hf_v \tag{5.1}$$

Here, hv', hv, and hf_v are the new photon energy, the incident photon energy, and the vibrational energy, respectively. In our design, the classical channel at 1351 nm is closest to the quantum channel at 1531 nm. The maximum gain of Raman scattering is known to be within 13 THz from the pump signal. So, the frequency of the classical channel is:

$$v = \frac{3 * 10^8 \text{ m/s}}{1.351 * 10^{-6}\ m} = 2.22 * 10^{14}\ Hz \tag{5.2}$$

and the stokes-shift frequency is:

$$v' = (22.2 - 1.3)\ 10^{13} = 2.09 *\ 10^{14} \tag{5.3}$$

Therefore, the Stokes-shift will correspond to wavelength:

$$\lambda = \frac{3 * 10^{8}}{2.09 *\ 10^{14}} = 1435\ nm \tag{5.4}$$

To verify the effect of Raman Stokes-shift in our architecture, we set the pumps of the classical channels to launch 0 dBm at 1351, 1331, 1311 and 1291 nm; then, we observed the Raman scattering Stoke-shift. The maximum power gain of the classical channels 1331 and 1351 nm occurred at 1415 and 1435 nm, respectively; also, the peak gain power of the 1311 and 1291 nm channels occurred before at 1389 and 1367 nm, respectively Figure 5.4. Thus, in our design, the classical signals have a minimum effect on the quantum channels.

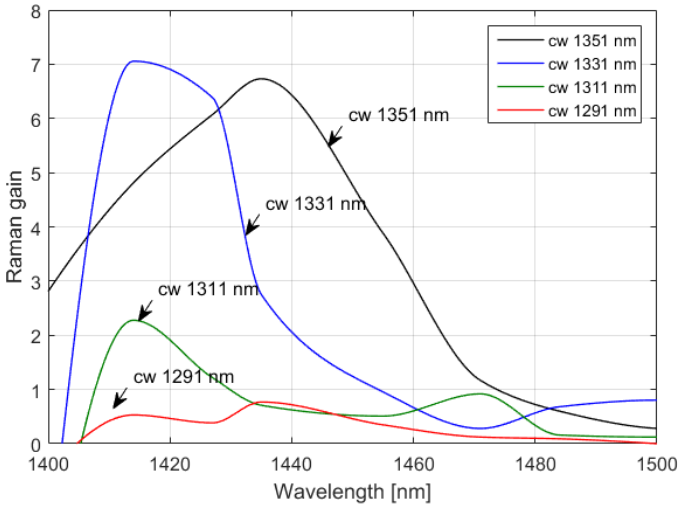

Figure 5.4. Shows the range of Raman gain (in arbitrary unit) caused by the pump of the classical channels. The maximum Raman gain of the 1351 nm channel occurs at a wavelength of 1435 nm. All the major noise of the classical channels occurred before the wavelengths of the quantum channels.

Also, we varied the separation between the channels to observe the noise reaching the quantum signals. We varied the spacing between the highest classical channel

wavelength (1351 nm) and the lowest quantum channel wavelength (1511 nm). We note that the noise in the quantum channels increases as the classical channel gets closer to the quantum signals Figure 5.5. Therefore, in our architecture, Raman Stokes-shift from the classical channels has less impact on the quantum channels.

5.6 Entanglement Distribution in an Optical Access Network

Let us consider entanglement distribution and classical communication in an access network. The EPR source, which is located in the access network, has direct communication with all users through the optical network switch. Using a laser with pump power of -99 dBm, we set up the wavelength of the laser in the SPDC to create two entangled states set at 1531 nm and 1571 nm Figure 5.6.

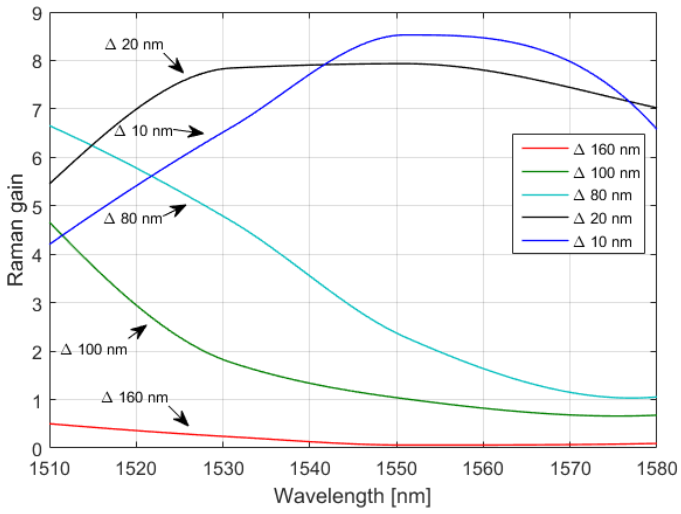

Figure 5.5. Shows the noise (in arbitrary units) caused by the classical channels as they get closer to the quantum channels. The lowest power gain occurs at the highest channel separation.

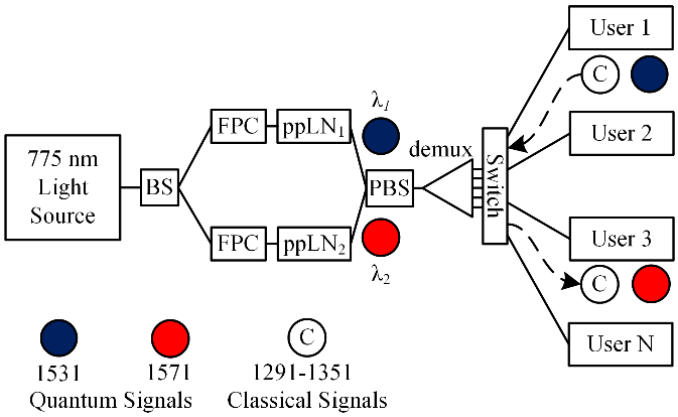

Figure 5.6. This diagram illustrates the direct entanglement distribution in the access network. The output states of the process of SPDC are demultiplexed and sent to the optical network switch and then to the end users. Classical communication signals between users are routed through the optical switch.

A WDM multiplexer carries the signals from the EPR source to the network switch. Then, the switch forwards the entangled states to the end users. The insertion losses in the CWDM multiplexer and the optical switch are 1.5 dBm/km and 1 dBm, respectively. This results in a slight decrease in the coincidence rates [67]. We used the O-band between 1271 nm and 1351 nm for the classical communication. The extra connections in the optical switch routes the classical communication between the users [66] within the access network. Since this access network has a short distance with few components, it has a low insertion loss close to 3 dBm.

5.7 Entanglement in Metropolitan Optical Network

We based the core network on ITU-T G.694.2 CWDM that contains a grid wavelength range between 1270 nm and 1610 nm. This spectral grid has 18 channels based on a space of 20 nm between the channels. We designate the wavelengths between 1271 nm and 1351 nm for classical communication, which launches signals at a power of 0 dBm.

We also include wavelengths 1511 nm and 1571 nm for the quantum communications. We setup the EPR source as a centralized node for entanglement distribution in the entire MON. Users in the same or different access networks request to share entanglement pairs for establishing secret keys using entanglement-based and entanglement-assisted quantum key distribution. When the EPR source receives a request, it creates entangled states by the process of SPDC in 1531-1571 nm or 1511-1551 nm, which correspond to CWDM channels. The output states travel from the EPR access network to the CWDM-based backbone via the local ROADM. Then, the EPR source remotely reconfigures the MEMS optical switches in the ROADMs to drop the wavelengths of the entangled states in the target access networks. Then, they pass through the AN/ROADM multiplexer. Then, the signals are demultiplexed to the network switch. Finally, the optical switch transmits the states to the end users Figure 5.7. Using the dedicated and authenticated classical channel of each access network, users establish secret keys using quantum key distribution protocols.

5.8 Simulation and Results

We designed and simulated our architecture using the optical communication system OptiSystem. In the design of the metropolitan optical network, we assume that the distance between neighboring backbone nodes is 4 km and the distance between the backbone node and the access network switch is 3.5 km. Also, we assume that the distance between the access network switch and the end users is 1 km. We estimate the insertion loss in the network based on a loss budget of 30 dBm [71]. Each access network has different insertion loss because of the centralized EPR source. The major insertion loss in

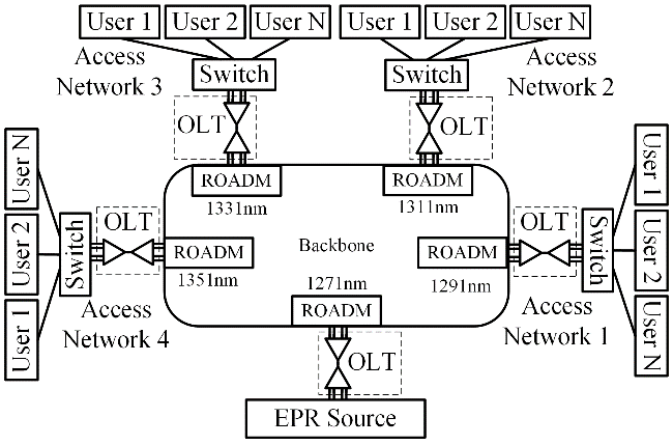

Figure 5.7. This diagram shows the centralized EPR source for entanglement distribution in MON. Quantum signals sent from the EPR travel in the backbone network are then dropped in the designated access network by the ROADM. Remotely reconfiguring the optical switches in the ROADM causes the wavelength of the entangled state to pass or drop. The wavelength of the classical channel is fixed for each access network and used for classical communication between users in different access networks.

the first access network results from two backbone nodes, fiber optic attenuation, and the access network switch. Therefore, the total insertion loss in the first access network is 13.22 and 10.6 dBm for the classical and quantum channels, respectively. In the second access network, the signals travel through three backbone nodes and double the distance of the first access network. The total insertion loss of the second access network is 18.5 and 15.4 dBm for classical and quantum channels, respectively. The insertion loss for the entire access network in the MON is provided in Table 5.1.

Table 5.1 Insertion loss for every access network in MON.

Network	No. ROADM	Loss C ch (dBm)	Loss Q ch (dBm)
AN-1	2	13.22	10.6
AN-2	3	18.5	15.4
AN-3	4	23.78	20.2
AN-4	5	29.06	25

The maximum insertion loss occurs in the fourth access network as the signals travel the longest distance and pass through several backbone nodes. The largest insertion loss in this network is tolerable as it falls below the acceptable 30 dBm loss budget. Adding new access networks results in insertion loss greater than 30 dBm in the new access networks. However, increasing the number of users in each access network has no effect on the insertion loss of the access networks. Consequently, the overall performance of the network remains unchanged. In Figure 5.8, we show the optical noise-to-signal ratio (ONSR) with respect to a different channel spacing between the classical and the quantum channels. The spacing in our architecture shows better ONSR because the classical signals have less impact on the quantum channels. Figure 5.9 shows the power of the signals measured at the last access network for fiber lengths of 20, 40 and 80 km.

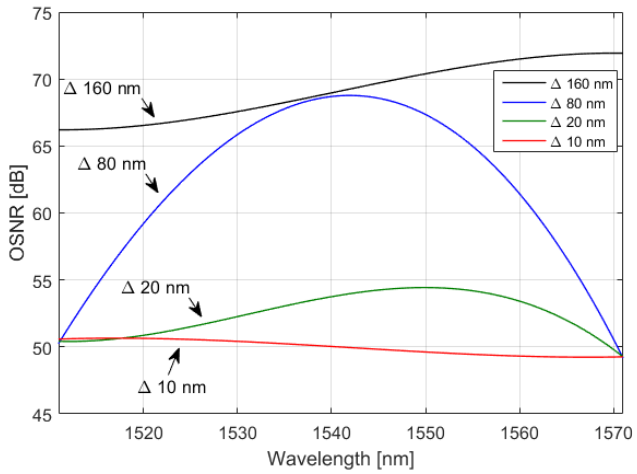

Figure 5.8. Shows the optical signal-to-noise ratio in the quantum channels with respect to different spacing to the wavelength of the classical signals. The optical signal-to-noise ratio in the quantum channels is shown with respect to different spacing to the wavelength of the classical signals.

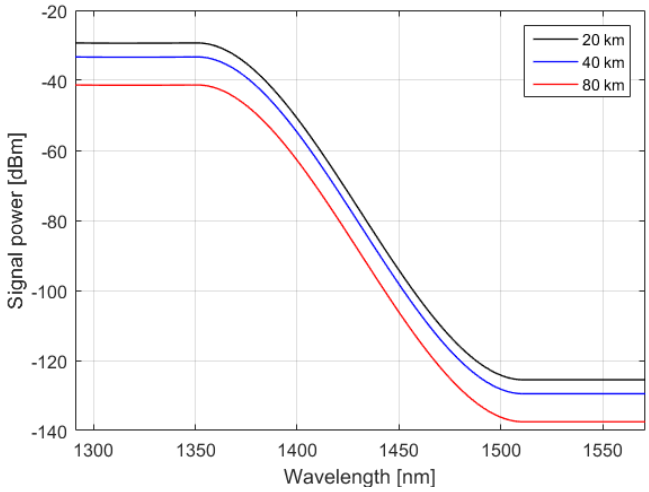

Figure 5.9. Shows the power of the signals of the classical and the quantum channels at the last access network and under different 20, 40 and, 80 km fiber lengths. Note that the drop between 1351 nm to 1511 nm indicates the spacing between the classical and the quantum channels.

Also, we show the bit error rate in Figure 5.10 with respect to the length of the fiber optic. The fiber attenuation loss decreases the signal power, which increases the bit error rate. It is possible to amplify the classical signal to reduce the BER and increase the signal traveling distance. However, there is no equivalent quantum amplifier quantum due to the no-cloning theorem [6].

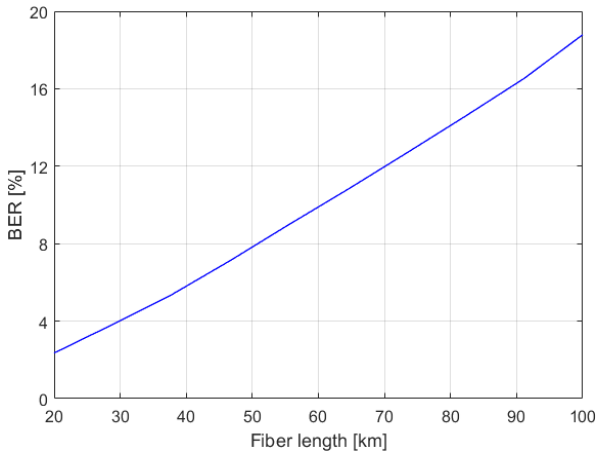

Figure 5.10. Shows the bit error rate of the classical channels for fiber length between 20 and 100 km.

We compare our network with the reference work in [66] using the same parameters in Table 1 [66]. We reduced the overall network loss and increased the number of the access networks from three to four Figure 5.11. Also, we considered a centralized EPR source to serve the entire MON instead of local EPR sources. The design of our ROADM provides a dynamic adding, dropping, or passing of the quantum wavelengths at each backbone node. In addition, the assigned classical channel provides a private communication between the access networks.

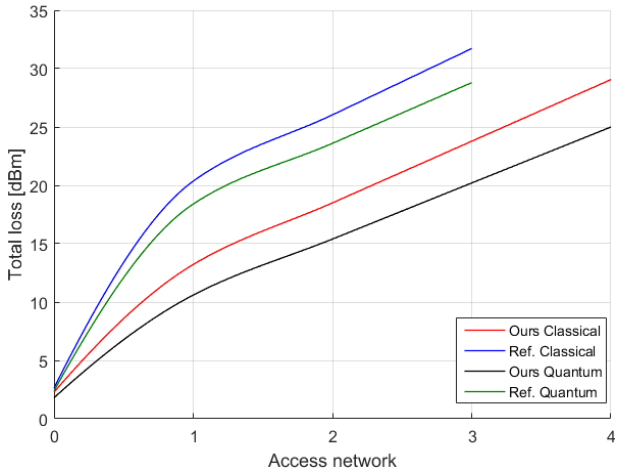

Figure 5.11. Comparison between our network and the reference work. We reduced the network loss and increased the number of access networks from three to four within the acceptable network signal loss.

CHAPTER 6: CONCLUSION

In this thesis, we presented a deterministic and efficient three-party quantum key distribution protocol to establish a secret key between two untrusted to each other users by a third party. The protocol distributes a secret key using a quantum channel that comprises two maximally entangled states and one two-particles von Neumann measurement. We introduced the parity bit of the entangled spins to help in preparing the secret states by applying two controlled-NOT gates. Also, we made the receivers introduce an ancillary state to their system. As a result, the users successfully reconstruct the target states after applying a controlled-NOT followed by one of the controlled-U gates. We discussed the security of our protocol and provided a method for privacy amplification. Also, we compared our protocol with the related protocols in the literature in terms of the intrinsic efficiency. The protocol is exact and deterministic; it distributes a secret key of d qubits to two parties by $2d$ entangled pairs and on average d bits of classical communication with the help of the introduced ancillary states. Also, we presented a quantum entanglement distribution in metropolitan optical networks. The centralized entanglement source serves all the users in the network. It creates entangled pairs with wavelengths that correspond to channels in the CWDM. By specifying the wavelengths to drop or pass at each backbone node, we provided a dynamic entanglement distribution for the entire network. Quantum and classical signals travel in the same fiber optic within different spectral bands. The maximum insertion loss in the network is 25 and 29 dBm for the quantum and the classical channels, respectively, which falls below the acceptable 30 dB budget loss.

REFERENCES

[1] G. S. Vernam, “Cipher Printing Telegraph Systems For Secret Wire and Radio Telegraphic Communications,” *Trans. Am. Inst. Electr. Eng.*, vol. XLV, no. 1, pp. 295–301, Jan. 1926.

[2] C. E. Shannon, “Communication Theory of Secrecy Systems*,” *Bell Syst. Tech. J.*, vol. 28, no. 4, pp. 656–715, Oct. 1949.

[3] C. H. Bennett and G. Brassard, “Quantum cryptography: Public key distribution and coin tossing,” in *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, Bangalore, India, Dec. 1984.

[4] A. K. Ekert, “Quantum cryptography based on Bell’s theorem,” *Phys. Rev. Lett.*, vol. 67, no. 6, pp. 661–663, Aug. 1991.

[5] P. W. Shor, “Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer,” *SIAM J. Comput.*, vol. 26, no. 5, pp. 1484–1509, Oct. 1997.

[6] W. K. Wootters and W. H. Zurek, “A single quantum cannot be cloned,” *Nature*, vol. 299, no. 5886, pp. 802–803, Oct. 1982.

[7] M. Alshowkan and K. M. Elleithy, “Deterministic and Efficient Quantum Key Distribution Using Entanglement Parity Bits and Ancillary Qubits,” *IEEE Access*, vol. 5, no. 99, pp. 25565–25575, Nov. 2017.

[8] M. Alshowkan and K. Elleithy, “Quantum Entanglement Distribution for Secret Key Establishment in Metropolitan Optical Networks,” in *2016 IEEE International Conference on Networking, Architecture and Storage (NAS)*, Long Beach, CA, USA, Aug. 2016.

[9] C. H. Bennett *et al.*, “Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels,” *Phys. Rev. Lett.*, vol. 70, no. 13, pp. 1895–1899, Mar. 1993.

[10] H.-K. Lo, “Classical-communication cost in distributed quantum-information processing: A generalization of quantum-communication complexity,” *Phys. Rev. A*, vol. 62, no. 1, p. 12313, Jun. 2000.

[11] A. K. Pati, “Minimum classical bit for remote preparation and measurement of a qubit,” *Phys. Rev. A - At. Mol. Opt. Phys.*, vol. 63, no. 1, pp. 1–3, Dec. 2001.

[12] C. H. Bennett *et al.*, “Remote State Preparation,” *Phys. Rev. Lett.*, vol. 87, no. 7, p. 77902, Jul. 2001.

[13] A. Abeyesinghe and P. Hayden, “Generalized remote state preparation: Trading cbits, qubits, and ebits in quantum communication,” *Phys. Rev. A*, vol. 68, no. 6, p. 62319, Dec. 2003.

[14] I. Devetak and T. Berger, “Low-Entanglement Remote State Preparation,” *Phys. Rev. Lett.*, vol. 87, no. 19, p. 197901, Oct. 2001.

[15] B. Zeng and P. Zhang, “Remote-state preparation in higher dimension and the

parallelizable manifold S^(n-1)," *Phys. Rev. A*, vol. 65, no. 2, p. 22316, Jan. 2002.

[16] G.-Y. Xiang *et al.*, "Remote preparation of mixed states via noisy entanglement," *Phys. Rev. A*, vol. 72, no. 1, p. 12315, Jul. 2005.

[17] D. W. Berry and B. C. Sanders, "Optimal Remote State Preparation," *Phys. Rev. Lett.*, vol. 90, no. 5, p. 57901, Feb. 2003.

[18] A. V. Gordeev *et al.*, "Numerical Modelling of Electron Flow in Plasma Switches," *Mat. Model.*, vol. 2, no. 9, pp. 40–48, Dec. 1990.

[19] B. Schumacher and M. D. Westmoreland, "Sending classical information via noisy quantum channels," *Phys. Rev. A*, vol. 56, no. 1, pp. 131–138, Jul. 1997.

[20] A. S. Holevo, "The capacity of the quantum channel with general signal states," *IEEE Trans. Inf. Theory*, vol. 44, no. 1, pp. 269–273, Jan. 1998.

[21] D. W. Leung and P. W. Shor, "Oblivious Remote State Preparation," *Phys. Rev. Lett.*, vol. 90, no. 12, p. 127905, Mar. 2003.

[22] A. Hayashi *et al.*, "Remote state preparation without oblivious conditions," *Phys. Rev. A*, vol. 67, no. 5, p. 52302, May 2003.

[23] M.-Y. Ye *et al.*, "Faithful remote state preparation using finite classical bits and a nonmaximally entangled state," *Phys. Rev. A*, vol. 69, no. 2, p. 22310, Feb. 2004.

[24] M. G. A. Paris *et al.*, "Remote state preparation and teleportation in phase space," *J. Opt. B Quantum Semiclassical Opt.*, vol. 5, no. 3, pp. S360–S364, Jun. 2003.

[25] Z. Kurucz *et al.*, “Continuous variable remote state preparation,” *Phys. Rev. A*, vol. 72, no. 5, p. 52315, Nov. 2005.

[26] Q. Zhou *et al.*, “Remote Preparation of Arbitrary Two-Particle Quantum State in Noisy Environments,” in *2012 Symposium on Photonics and Optoelectronics*, Shanghai, China, May 2012.

[27] L. Yi-Min *et al.*, “Remote Preparation of Three-Particle GHZ Class States,” *Commun. Theor. Phys.*, vol. 49, no. 2, pp. 359–364, Feb. 2008.

[28] D. Wang *et al.*, “Remote preparation of a class of three-qubit states,” *Opt. Commun.*, vol. 281, no. 4, pp. 871–875, Feb. 2008.

[29] J.-M. Liu and Y.-Z. Wang, “Remote preparation of a two-particle entangled state,” *Phys. Lett. A*, vol. 316, no. 3–4, pp. 159–167, Sep. 2003.

[30] H. Kui and S. Shou-Hua, “Classical Communication Cost and Probabilistic Remote Preparation of Four-Particle Entangled W State,” *Commun. Theor. Phys.*, vol. 51, no. 3, pp. 411–418, Mar. 2009.

[31] S.-Y. Ma and M.-X. Luo, “Efficient remote preparation of arbitrary two- and three-qubit states via the χ state,” *Chinese Phys. B*, vol. 23, no. 9, p. 90308, Sep. 2014.

[32] D. Wang *et al.*, “Joint remote state preparation of arbitrary two-qubit state with six-qubit state,” *Opt. Commun.*, vol. 284, no. 24, pp. 5853–5855, Dec. 2011.

[33] Q.-Q. Chen *et al.*, “Joint remote preparation of an arbitrary three-qubit state via EPR-type pairs,” *Opt. Commun.*, vol. 284, no. 10–11, pp. 2617–2621, May 2011.

[34] Q.-Q. Chen *et al.*, "Probabilistic joint remote preparation of a two-particle high-dimensional equatorial state," *Opt. Commun.*, vol. 284, no. 20, pp. 5031–5035, Sep. 2011.

[35] B. S. Choudhury and A. Dhara, "Joint remote state preparation for two-qubit equatorial states," *Quantum Inf. Process.*, vol. 14, no. 1, pp. 373–379, Jan. 2015.

[36] L.-W. Chang *et al.*, "Joint remote preparation of an arbitrary five-qubit Brown state via non-maximally entangled channels," *Chinese Phys. B*, vol. 23, no. 9, p. 90307, Sep. 2014.

[37] Y.-X. Huang and M.-S. Zhan, "Remote preparation of multipartite pure state," *Phys. Lett. A*, vol. 327, no. 5–6, pp. 404–408, Jul. 2004.

[38] H. Yan-Xia *et al.*, "A Peculiar Tripartite Entangled State," *Chinese Phys. Lett.*, vol. 20, no. 9, pp. 1423–1425, Sep. 2003.

[39] Y.-F. Yu *et al.*, "Preparing remotely two instances of quantum state," *Phys. Lett. A*, vol. 310, no. 5–6, pp. 329–332, Apr. 2003.

[40] D. Hong-Yi *et al.*, "Classical Communication Cost and Remote Preparation of Multi-qubit with Three-Party," *Commun. Theor. Phys.*, vol. 50, no. 1, pp. 73–76, Jul. 2008.

[41] D. Hong-Yi *et al.*, "Remote preparation of an entangled two-qubit state with three parties," *Chinese Phys. B*, vol. 17, no. 1, pp. 27–33, Jan. 2008.

[42] W. Zhang-Yin *et al.*, "Controlled Remote State Preparation," *Commun. Theor. Phys.*, vol. 52, no. 2, pp. 235–240, Aug. 2009.

[43] H. Kui *et al.*, “Multiparty-Controlled Remote Preparation of Two-Particle State,” *Commun. Theor. Phys.*, vol. 52, no. 5, pp. 848–852, Nov. 2009.

[44] Y. Xia *et al.*, “Multiparty remote state preparation,” *J. Phys. B At. Mol. Opt. Phys.*, vol. 40, no. 18, pp. 3719–3724, Sep. 2007.

[45] B.-S. Shi and A. Tomita, “Remote state preparation of an entangled state,” *J. Opt. B Quantum Semiclassical Opt.*, vol. 4, no. 6, pp. 380–382, Dec. 2002.

[46] N.-R. Zhou *et al.*, “Three-party remote state preparation schemes based on entanglement,” *Quantum Inf. Process.*, vol. 13, no. 2, pp. 513–526, Feb. 2014.

[47] P. Agrawal *et al.*, “Exact remote state preparation for multiparties using dark states,” *Int. J. Quantum Inf.*, vol. 1, no. 3, pp. 301–319, Sep. 2003.

[48] M.-X. Luo *et al.*, “Deterministic remote preparation of an arbitrary W -class state with multiparty,” *J. Phys. B At. Mol. Opt. Phys.*, vol. 43, no. 6, p. 65501, Mar. 2010.

[49] X.-Q. Xiao *et al.*, “Joint remote state preparation of a qubit state via a W state using single-atom rotation operations,” in *The 2014 2nd International Conference on Systems and Informatics (ICSAI 2014)*, Shanghai, China, Nov. 2014.

[50] Z.-H. Zhang *et al.*, “Joint remote state preparation between multi-sender and multi-receiver,” *Quantum Inf. Process.*, vol. 13, no. 9, pp. 1979–2005, Sep. 2014.

[51] N. A. Peters *et al.*, “Remote State Preparation: Arbitrary Remote Control of Photon Polarization,” *Phys. Rev. Lett.*, vol. 94, no. 15, p. 150502, Apr. 2005.

[52] X. Peng *et al.*, “Experimental implementation of remote state preparation by nuclear

magnetic resonance," *Phys. Lett. A*, vol. 306, no. 5–6, pp. 271–276, Jan. 2003.

[53] J. Ye *et al.*, "Remote Preparation of Photon Polarization State via Einstein-Podolsky-Rosen Channel," in *2009 Symposium on Photonics and Optoelectronics*, Wuhan, China: IEEE eXpress Conference Publishing, Aug. 2009.

[54] M. Alshowkan *et al.*, "A new algorithm for three-party Quantum key distribution," in *Third International Conference on Innovative Computing Technology (INTECH 2013)*, London, UK: IEEE, Aug. 2013.

[55] F. Zamani and P. K. Verma, "A QKD protocol with a two-way quantum channel," in *2011 Fifth IEEE International Conference on Advanced Telecommunication Systems and Networks (ANTS)*, Dec. 2011.

[56] M. Alshowkan and K. Elleithy, "Authenticated multiparty secret key sharing using quantum entanglement swapping," in *Proceedings of the 2014 Zone 1 Conference of the American Society for Engineering Education*, Bridgeport, CT, USA, Apr. 2014.

[57] M. Alshowkan and K. Elleithy, "Secret key sharing using entanglement swapping and remote preparation of quantum state," in *IEEE Long Island Systems, Applications and Technology (LISAT) Conference 2014*, Farmingdale, NY, USA, May 2014.

[58] Sheng-Tzong Cheng *et al.*, "Quantum communication for wireless wide-area networks," *IEEE J. Sel. Areas Commun.*, vol. 23, no. 7, pp. 1424–1432, Jul. 2005.

[59] M. Naseri, "Revisiting Quantum Authentication Scheme Based on Entanglement Swapping," *Int. J. Theor. Phys.*, vol. 55, no. 5, pp. 2428–2435, May 2016.

[60] M. Alshowkan and K. Elleithy, "Quantum mutual authentication scheme based on Bell state measurement," in *2016 IEEE Long Island Systems, Applications and Technology Conference (LISAT)*, Farmingdale, NY, USA, Apr. 2016.

[61] J. L. Carter and M. N. Wegman, "Universal classes of hash functions," *J. Comput. Syst. Sci.*, vol. 18, no. 2, pp. 143–154, Apr. 1979.

[62] P. Kok and S. L. Braunstein, "Postselected versus nonpostselected quantum teleportation using parametric down-conversion," *Phys. Rev. A*, vol. 61, no. 4, p. 42304, Mar. 2000.

[63] X. Ma *et al.*, "Quantum key distribution with entangled photon sources," *Phys. Rev. A*, vol. 76, no. 1, p. 12307, Jul. 2007.

[64] T. Jennewein *et al.*, "Experimental proposal of switched 'delayed-choice' for entanglement swapping," *Int. J. Quantum Inf.*, vol. 3, no. 1, pp. 73–79, Mar. 2005.

[65] H. Yuan *et al.*, "Optimizing resource consumption, operation complexity and efficiency in quantum-state sharing," *J. Phys. B At. Mol. Opt. Phys.*, vol. 41, no. 14, p. 145506, Jul. 2008.

[66] A. Ciurana *et al.*, "Entanglement Distribution in Optical Networks," *IEEE J. Sel. Top. Quantum Electron.*, vol. 21, no. 3, pp. 37–48, May 2015.

[67] I. Herbauts *et al.*, "Demonstration of active routing of entanglement in a multi-user network," *Opt. Express*, vol. 21, no. 23, p. 29013, Nov. 2013.

[68] N. A. Peters *et al.*, "Dense wavelength multiplexing of 1550 nm QKD with strong

classical channels in reconfigurable networking environments," *New J. Phys.*, vol. 11, no. 4, p. 45012, Apr. 2009.

[69] B. Qi *et al.*, "Feasibility of quantum key distribution through a dense wavelength division multiplexing network," *New J. Phys.*, vol. 12, no. 10, p. 103042, Oct. 2010.

[70] P. Eraerds *et al.*, "Quantum key distribution and 1 Gbps data encryption over a single fibre," *New J. Phys.*, vol. 12, no. 6, p. 63027, Jun. 2010.

[71] D. Lancho *et al.*, "QKD in Standard Optical Telecommunications Networks," in *Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering*, vol. 36 LNICST, A. Sergienko, S. Pascazio, and P. Villoresi, Eds. Naples, Italy: Springer, 2010, pp. 142–149.